

# EXHIBIT B

**MOORE**  
**INTERNATIONAL LAW PLLC**

**INTERNATIONAL LEGAL MATTERS**

**ROCKEFELLER CENTER**  
**45 ROCKEFELLER PLAZA, 20<sup>TH</sup> FLOOR**  
**NEW YORK, NEW YORK 10111 USA**  
**TELEPHONE: + (212) 332-3474**  
**FACSIMILE: + (212) 332-3475**  
**WWW.MILOPC.COM**

WRITER: SCOTT MICHAEL MOORE  
[SMM@MILOPC.COM](mailto:SMM@MILOPC.COM)  
LICENSED & ADMITTED  
SUPREME COURT OF THE UNITED STATES OF AMERICA  
U.S. COURT OF APPEALS FOR THE FEDERAL CIRCUIT  
U.S. COURT OF INTERNATIONAL TRADE  
OTHER U.S. FEDERAL COURTS  
STATES OF NEW YORK & MICHIGAN ONLY  
LONDON COURT OF INTERNATIONAL ARBITRATION

Via Email

17 July 2020

Greenberg Traurig  
David G. Barger, Esq. (bargerd@gtlaw.com)

Re: *El Omari v. Buchanan, et al*, 20-cv-2601 (S.D.N.Y.)

Dear Mr. Barger:

This letter is sent pursuant to Judge Marrero's Practice Rule II(B)(1), in response to your pre-motion to dismiss letter on behalf of the KARV Defendants, dated July 13, 2020.<sup>1</sup>

**Other similar litigation involving the KARV Defendants** – See Amended Compl., (AC), Par. 27, *Ras Al Khaimah Investment Authority v. Farhad Azima*, Claim No. CR-2016-002798. Similarities between the AC and RAKIA include instructions from Saud to Buchanan and associates to “target” and “go after” Azima, like El Omari, (Par. 33, 34, 37, 255c), use of spear-phishing emails to illegally access Azima’s emails, similar to the “Samantha Alison” scheme (Par. 343, 350), and the email of August 16, 2016 from Buchanan to Frank and Handjani, connecting them to Azima’s hacked emails (Par. 350). (RAKIA Judg., May 20, 2020, excerpts, Exh. 1.).<sup>2</sup> Also, Frank and KARV created the “View from the Window” involving Azima (RAKIA Judg., Par. 37, 301), and Buchanan’s email of July 19, 2015, to “go after FA subject to guidance from AF [Andrew Frank].” (RAKIA Judg., Par. 288). See communication hierarchy, Exh. 2. See also AC’s Iran sanction violation protection/retaliation consistency with recently filed *USA v. Funds in the amount of 73,293,750 AED (Approximately \$20 Million) in the possession and control of Ras Al Khaimah Investment Authority (RAKIA) et al.*, Case No. 20-cv-126 (D. Alaska), on June 3, 2020, Exh. 3.

**I. The KARV Defendants cannot invoke common law sovereign immunity** - You contend as alleged agents of Saud, the KARV Defendants enjoy common law sovereign immunity. This is an unsupported leap from the AC’s alleged private illegal actions of the KARV Defendants to lawful official duties. *Moriah v. Bank of China Ltd.*, 107 F. Supp. 3d 272, 277 (S.D.N.Y. 2015); *In re Doe*, 860 F.2d 40, 45 (2d Cir. 1988); *Samantar v. Yousuf*, 560 U.S. 305 (2010).<sup>3</sup>

**II. El Omari sufficiently plead a civil RICO claim** - You parse the AC, and ignore RAKIA. The false FARA filings are plead to constitute mail and wire fraud predicates (AC, Par. 123-124), the “Samantha Alison’s” emails and Skypes as wire fraud predicates (AC, Par. 124), and witness

<sup>1</sup> On July 1, 2020, Plaintiff inquired if you would be willing to share information about whether KARV initiated any independent review of the allegations in the AC. No response to date.

<sup>2</sup> Excerpts include discussions of party submissions, testimony, documentary evidence, and findings.

<sup>3</sup> The acts complained of in the AC are subsequent and continuing after El Omari’s prior litigation you cite.

17 July 2020

Page 2 of 3

retaliation and conspiracy predicates (AC, Par. 125, 126). Wire fraud predicate - Pointing to AC, Par. 137-151, 124, you contend the “Samantha Alison” - KARV Defendants connection is insufficient under Rule 9(b). However, KARV’s history of harassment, Frank and Handjani’s relationship with RAK, El Omari’s experience with RAK harassment, Frank’s ability to use a “back stop,” and the similarity to *RAKIA*, show that there is reason to believe “Samantha Alison” is related to the KARV Defendants. Further, they are technologically savvy, and to establish that relationship further would be peculiarly within the defendant’s knowledge. *DiVittorio v Equidyne Extractive Indus., Inc.*, 822 F2d 1242, 1247 (2d Cir 1987). El Omari’s disclosed information about this case and related matters is valuable property. (AC, Par. 148). Each of the 13 emails (AC, Par. 140, 141) and 5 Skype interviews (AC, Par. 143) constitute separate wire fraud predicate acts. El Omari gave away critical information because of these misrepresentations. *Palatkevich v Choupak*, 152 F Supp 3d 201 (S.D.N.Y. 2016). You also assert in talking to “Samantha Alison,” El Omari would expect the information to be made public. However, El Omari plead he was promised confidentiality (AC, Par. 139, 140, 143 147), and he relied on such for the information not to be public. (AC, Par. 147).

Witness retaliation predicate - You assert lack of allegations that the KARV Defendants knew of contact by the CIA and other activities, pointing to AC, Par. 37, 125-6. But see *Palatkevich*. See also the similar pattern in *RAKIA*, such as the “View from the Window” and the email of August 16, 2016 connecting the KARV Defendants to Azima’s hacked emails, showing the omniscient nature of the KARV Defendants’ knowledge and activity about their targets.

FARA regulatory filings and mail/wire fraud - You assert the FARA regulatory filings do not seek to obtain property from El Omari, and the fraud scheme is not plead with particularity, pointing to AC, Par. 64. The KARV Defendants directly benefited from the scheme of FARA misrepresentations by payment in return for protection of Saud: PR contract awards to Frank and Iran Oil Scheme profits to Handjani. (AC, Par. 65, 66). The KARV Defendants could not act as alleged without the false FARA filings. Moreover, if a plaintiff alleges two or more predicate acts, as here, the plaintiff need only suffer injury from one, e.g. injury from witness retaliation or “Samantha Alison.” *Hecht v. Commerce Clearing House, Inc.*, 897 F.2d 21, 23 (2d Cir. 1990).

Continuity element - You contend there are no “open-ended” or “closed-ended” facts. However both closed-ended and the “continued, or the threat of continued activity” requirements are met because the FARA falsification has been continuing since 2013, and the “Samantha Alison” scheme concerns ongoing protection of Saud and ongoing litigations. “Samantha Alison” had been trying to get information from El Omari through misrepresentation. *Azrielli v Cohen Law Offices*, 21 F3d 512, 521 (2d Cir 1994). “Continuous” and “threat of continuous” are supplemental, rather than complementary requirements. *H.J. Inc. v. Northwestern Bell Co.*, 492 U.S. 229, 242 (1989).

Injury and proximate cause - You assert lack of meeting a clear and definite standard in AC, Par. 125, and lack of a direct relation causation requirement. You also argue El Omari’s termination in AC, Par. 38, is a substantial intervening factor. However, a plaintiff only needs to suffer direct injury from one of the predicate acts. *Hecht*, at 23. See the “Samantha Alison” scheme and the direct information and financial injury in AC, Par. 148, 149.

### **III. El Omari sufficiently plead a claim of defamation per se**

You opine lack of connection to the IO Article. However, all who take part in the procurement, composition and publication of a libel are responsible in law and equally so. *Restis v. American Coalition Against Nuclear Iran, Inc.*, 53 F.Supp.3d 705, 716-717 (S.D.N.Y. 2014). AC, Par. 24, made such an allegation. See *Palatkevich*. Note similarity between the KARV Defendants’ conduct alleged here with *RAKIA*. See e.g., “View from the window” and emails between Buchanan and

**MOORE**

**INTERNATIONAL LAW PLLC**

17 July 2020

Page 3 of 3

Handjani (*RAKIA* Judgment, P. 283-288), in particular, “to go after FA subject to guidance from AF [Andrew Frank]. … will speak to AF tomorrow and fill you in.” “Talking to the boss now. He wants me … to coordinate with you.” (*RAKIA* Judg., P. 288).

You contend that the AC fails to plead defamation per se. Defamation per se absolves a plaintiff from proving special harm where a statement “tends to injure another in his or her trade, business, or profession.” *Medcalf v. Walsh*, 938 F.Supp.2d 478, 487 (S.D.N.Y. 2013); *Fuji Photo Film U.S.A., Inc. v. McNulty*, 669 F.Supp.2d 405, 411 (S.D.N.Y. 2009). The AC alleges the IO article and its advertisement, attached as AC exhibits, reports that El Omari committed a serious crime, a billion dollar RAKIA related fraud, a place where El Omari never worked, and with its CEO whom El Omari didn’t know personally. (AC, Par. 19, 19a, 19b, 19c, 19c-d, and 25).

You argue the words, “The investment authority believes that…” means opinion. Here, the specific language about El Omari’s RAKIA billion dollar fraud and connection with RAKIA’s CEO has a precise meaning which is readily understood, is capable of being proven true or false, the full context of the communication in which the statement appears are such as to signal readers that what is being read is likely to be fact, not opinion. *Lan Sang v. Ming Hai*, 951 F.Supp.2d 504, 517, 519 (S.D.N.Y. 2013); *Restis*, at 718.

Lastly, you contend that El Omari is a public figure. El Omari denies he is a public figure for purposes of defamation. Nonetheless, El Omari did allege “reckless disregard” at AC, Par. 25.

#### **IV. El Omari sufficiently plead a claim under the CFAA**

You opine that communicating is not unauthorized access to a computer. The AC alleges the computer emails and Skype were intentionally sent to El Omari, and used identity misrepresentation and a promise of confidentiality, to gain access to El Omari through his computer. (AC, Par. 140-143). This was “spear-phishing” El Omari. (*RAKIA* Judgment, Par. 36).

You contend that the threshold value of a \$5,000 loss has not been plead. See AC, Par. 149. El Omari’s attorney fees and investigation costs in response to “Samantha Alison” have easily exceeded \$5,000. “[T]he costs of investigating security breaches constitute recoverable ‘losses.’” *Sell It Social, LLC v. Strauss*, 15-cv-970, Mem. and Order, March 8, 2018, p. 8 (S.D.N.Y. 2018).

Lastly, you argue lack of a connection to “Samantha Alison.” See AC, Par. 138, 139, and 143, and the above response to the RICO wire fraud predicate involving “Samantha Alison.” Also, note the “cease and desist letters” sent to the KARV Defendants (AC, Par. 138), were followed by “Samantha Alison” (AC, Par. 139) seeking “knowledge about allegations found in three lawsuits” (the instant, *RAKIA*, and *Sadeq*) (AC, Par. 143).

For all these reasons, El Omari will respectfully oppose your motion to dismiss.

Sincerely,

**MOORE INTERNATIONAL LAW PLLC**

BY: /s/ Scott M. Moore

Scott Michael Moore  
Attorney at Law  
Counsel for Plaintiff, Oussama El Omari

Attachments: Plaintiff’s Letter Exhibits1-3

Cc: Hon. Victor Marrero, U.S.D.J., via Email: ChambersNYSDMarrero@nysd.uscourts.gov

## PLAINTIFF'S EXHIBIT 1

**Neutral Citation Number: [2020] EWHC 1327 (Ch)**

**IN THE HIGH COURT OF JUSTICE  
BUSINESS AND PROPERTY COURTS  
OF ENGLAND AND WALES  
BUSINESS LIST (ChD)**

**Case No. HC-2016-002798**

Royal Courts of Justice  
Rolls Building, Fetter Lane, London EC4A 1NL

Date: 22 May 2020

**Before:**

**ANDREW LENON Q.C. (sitting as a Deputy Judge of the Chancery Division)**

**BETWEEN:-**

**RAS AL KHAIMAH INVESTMENT AUTHORITY**

**Claimant**

**- and -**

**FARHAD AZIMA**

**Defendant**

---

**APPROVED JUDGMENT**

---

**Hugh Tomlinson Q.C. and Edward Craven (instructed by Stewarts Law LLP) for the  
Claimant**

**Tim Lord Q.C. and Hugo Leith (instructed by Burlingtons LLP) for the Defendant**

**Hearing dates: 22<sup>nd</sup> - 24<sup>th</sup> January, 27<sup>th</sup> - 31<sup>st</sup> January, 3<sup>rd</sup> - 5<sup>th</sup> February, 12<sup>th</sup> - 14<sup>th</sup>  
February 2020**

**Date: 22 May 2020**

I direct that pursuant to CPR PD 39A para 6.1 no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

Covid-19 Protocol: This judgment was handed down by the judge remotely by circulation to the parties' representatives by email and release to Bailii. The date and time for hand-down is deemed to be 14.00 am on 22 May 2020.

**(6) The Project Update and its aftermath**

30. By late 2014 investigations were under way within RAK into the actions of Dr Massaad and his associates.
31. In January 2015 Stuart Page, a private investigator, was engaged by the Ruler to investigate what the Ruler feared was a plot between a member of his family and Dr Massaad aimed at destabilising his rulership.
32. In March 2015 Mr Page provided the Ruler with a report entitled RAK Project Update ("the Project Update") which was mainly concerned with Dr Massaad's activities but which also described how Mr Azima was managing a team of advisers in the US, hired by Dr Massaad, who were planning to spread allegations about human rights issues in RAK; their campaign had not yet been made public. Mr Page's agents who compiled the report said that they would be able to gather intelligence on the campaign team in order to monitor their progress and "attempt to contain or ruin their plans".
33. In around April 2015, the Ruler told Mr Buchanan that he wanted Mr Buchanan and other assistants to "target" Mr Azima. The Ruler directed his associates to bring charges against Mr Azima. The Ruler's associates discussed meeting to "coordinate our attack" on Mr Azima and Dr Massaad but persuaded the Ruler not to pursue this plan at that time.
34. In or around July 2015, the Ruler instructed another of his assistants, Naser Al Bustami, to "go after" Mr Azima. Mr Azima's case is that, just as Henry II's question "Will no one rid me of this turbulent priest?" led to the murder of Thomas Becket, so the Ruler's directions to "go after" Mr Azima led in due course to the hacking of Mr Azima's emails, whether or not this was the Ruler's express instruction.

**(7) The hacking of Mr Azima's emails**

35. A 'phishing' email is an email that seeks to trick the recipient into clicking on a hyperlink taking the user to a webpage that the criminal controls, or into downloading malicious software. A 'spear-phishing' email is a more targeted and sophisticated form of a 'phishing' email which indicates that the sender has purposely targeted the deception at that individual (as shown by the fact that the email has been constructed to include material pertinent to the recipient, or otherwise to be of more interest to them). The fact that the spear-phishing email contains material of particular interest to the targeted recipient makes it more likely to be effective in that the recipient is more likely to open the deceptive email and any further links it may contain.
36. It is common ground that in October 2015 Mr Azima received a number of spear-phishing emails. Mr Azima's case is that these spear-phishing emails led at the time to the hacking of his confidential email accounts, that the hacking was organised by agents acting on behalf of RAKIA and that consequently by late 2015 RAKIA had accessed his confidential emails and the evidence which it now relies on in support of its claims. RAKIA denies that it had anything to do with the spear-phishing emails and does not admit that the spear-phishing emails led to the hacking of Mr Azima's email accounts.

37. On 29 December 2015 a document called the “View from the Window” was drawn up by Andrew Frank, an employee of Karv Communications, a PR firm engaged by RAK. The document referred to Mr Azima as “having orchestrated, if not fully participated in numerous fraudulent activities” and to “companies being set up with Iranian nationals”. Mr Azima contends that this document shows that RAKIA had by this stage obtained access to Mr Azima’s confidential emails and data. This is disputed by RAKIA.

#### **(8) The Settlement Agreement**

38. On 2 March 2016 RAKIA, HeavyLift and Mr Azima entered into the Settlement Agreement. The Recitals to the Settlement Agreement read as follows:

“(A) By an agreement dated 12 April 2007, HeavyLift and RAK Airways PJSC (“RAK Airways”) entered into a joint venture (the “Joint Venture Agreement”) to establish an Aircraft Simulator and Training Facility at Ras Al Khaimah International Airport, located in Ras Al Khaimah, UAE (“RAK”);  
(B) RAKIA guaranteed the performance of RAK Airways under the Joint Venture Agreement;  
(C) HeavyLift, acting through Mr Azima, has asserted that RAK Airways owes HeavyLift for investments HeavyLift made in the joint venture pursuant to the Joint Venture Agreement;  
(D) RAKIA does not agree that there is any legal basis for any such claim;  
(E) Mr. Azima has recently provided negotiation assistance to RAKIA on an informal basis which RAKIA recognises and appreciates;  
(F) Each Party has the greatest of respect for the other Parties, and wishes to resolve all outstanding issues relating to the Joint Venture Agreement.”

39. Clause 1.1 required RAKIA to pay the sum of \$2.6 million in settlement of any claims that Mr Azima or HeavyLift might have had against RAKIA or another RAK entity:

“RAKIA will pay HeavyLift the sum of \$2,600,000 to resolve all claims which Mr Azima or HeavyLift may have against it or any other RAK Entity as further detailed in paragraph 3.1.”

40. RAKIA’s case is that it was deceived into entering the Settlement Agreement by fraudulent misrepresentations made by and on behalf of Mr Azima regarding the amount of HeavyLift’s investment, that the settlement sum of \$2.6m was intended to reflect the amount spent by HeavyLift in making its contribution to the Training Academy JV and that the true amount of HeavyLift’s investment was significantly smaller than this.

41. In exchange for the payment of \$2.6m, Mr Azima and HeavyLift agreed to relinquish

**(11) The downloading of the hacked material**

51. The dispute with Dr Massaad was not resolved. RAKIA admits to creating websites attacking Dr Massaad a few days after the July 2016 meeting and shortly after those sites were created, in early August 2016, blogging websites began appearing denigrating Mr Azima as a “fraud” and a “scammer” and linking to websites containing Mr Azima’s confidential emails which appeared at around the same time.
52. There is an issue as to how these blogging web sites came to the attention of RAKIA. RAKIA’s case is that they were discovered by a journalist, Majdi Halabi, who drew them to the attention of Mr Page, by whom Mr Halabi had been allegedly asked to look out for references to Mr Azima on the internet. Mr Page is alleged to have communicated the information to Mr Gerrard and Mr Buchanan. Mr Azima contends that this version of events is fictitious, that Mr Halabi played no part in the discovery of the blogging web sites and that RAKIA’s account of the discovery of the blogging websites is designed to conceal RAKIA’s role in the hacking.
53. RAKIA subsequently instructed an independent third party, Northern Technology Inc. (“NTi”) to download the material from these links and others which were subsequently discovered and which RAKIA contends had been posted by unknown hackers. The material was downloaded by NTi in August and September 2016.
54. RAKIA’s case is that the subsequent analysis of the internet data established that, contrary to the Good Faith Clause, Mr Azima had in fact committed multiple acts of serious wrongdoing towards RAKIA and other RAK entities and that, as a result of that discovery, the present action was commenced on 30 September 2016.
55. On Mr Azima’s case, RAKIA already had access to the hacked data by late 2015 so that the downloading process in August/September 2016 was a charade.
56. On the same day as these proceedings were commenced (30 September 2016) Mr Azima brought proceedings against RAKIA in the US District Court for the District of Columbia alleging that RAKIA had hacked his computers. RAKIA challenged the proceedings on jurisdictional grounds. Its challenge failed in the US District Court but on 18 June 2019 the US Court of Appeals allowed RAKIA’s appeal and dismissed the US proceedings.
57. Mr Azima amended his defence in these proceedings on 18 July 2018 to allege that RAKIA was responsible for hacking his computers and emails and publishing their contents on the Internet and on 8 August 2019 was given permission to add a Counterclaim for damages and other relief arising out of the alleged hacking which was stayed pending final judgment on RAKIA’s claim.

## The witnesses

58. RAKIA served witness statements from twelve witnesses, nine of whom gave oral evidence. The evidence of two of the witnesses, Richard Garcia and Jessica Gray, who were involved in the downloading of data from the BitTorrent sites, was uncontroversial and admitted by Mr Azima without cross-examination.
59. The Ruler of RAK, Sheikh Saud bin Saqr Al Qasimi, provided a witness statement responding to Mr Azima's first witness statement but did not attend the hearing. RAKIA submitted that for the Ruler to attend the hearing or appear by video link would be incompatible with this constitutional role and status as sovereign ruler. It is regrettable that the Ruler chose not to attend the hearing or give evidence by video link as there were a number of issues on which he could have given relevant evidence. As the Ruler's witness statement was not tested by cross-examination, I do not propose to attach significant weight to it.
60. Jamie Buchanan was RAKIA's main witness. Between September 2014 and December 2019 when he took retirement, Mr Buchanan was the chief executive of Ras Al Khaimah Development LLC ("RAK Dev") which holds the assets and liabilities that were previously owned by RAKIA.
61. Counsel for Mr Azima submitted that Mr Buchanan gave dishonest evidence on a number of issues relating to Mr Azima's hacking claim. In relation to one matter, namely Mr Buchanan's claim to have been mistaken, until shortly before the trial, as to the authorship of the Project Update, which I address at paragraph 266 below, I consider that Mr Buchanan's evidence was disingenuous. I was not persuaded that Mr Buchanan's evidence was dishonest in other respects. He struck me as a generally reliable witness who gave his evidence in a measured way and was prepared to concede a number of points adverse to RAKIA's case that were put to him in cross examination.
62. Neil Gerrard is a former policeman and a partner in the firm of Dechert LLP which was instructed to assist with the investigation into Dr Massaad's alleged fraudulent activities which it has continued to work on to the present time. His witness statement dealt with his engagement by RAK, the meeting he had with Mr Azima in July 2016 and the events in August 2016 surrounding the downloading of the hacked material. He was cross-examined about his involvement with the questioning of detainees within RAK, in particular Karam Al Sadeq and Shahab Izadpanah. Allegations that Mr Gerrard had attempted, on behalf of RAK, to extort money from Mr Izadpanah and had offered Mr Izadpanah and Mr Al Sadeq to drop all charges against them if they confessed to charges implicating Dr Massaad were put to Mr Gerrard who denied them in forthright terms. On the basis of the material before me, I am not in a position to make any findings in relation to those allegations or other allegations of misconduct extraneous to the events in issue in these proceedings that were put to Mr Gerrard.
63. Counsel for Mr Azima submitted that Mr Gerrard gave dishonest evidence on key issues. He was also criticised for not referring to Mr Page and the Project Update in his witness statement. In my view, Mr Gerrard's witness statement should have dealt

with the Project Update which was a clearly relevant document and one which, as he accepted in cross-examination, was of concern to him when it was produced because it referred to the threat of a press campaign to smear RAK and its Ruler with human rights allegations. I do not, however, regard the omission to deal with the Project Update, or the other criticisms made of his evidence, as leading to the conclusion that I should treat Mr Gerrard as dishonest.

64. Stuart Page, also a former policeman and now the Chairman and majority shareholder of a business providing security and surveillance services, dealt in his witness statement with his engagement in RAK to assist with the investigations into Dr Massaad and the discovery of the hacked material. Counsel for Mr Azima submitted that Mr Page was a dishonest witness who lied about a number of matters. I consider that Mr Page was an unsatisfactory and unreliable witness. As set out in greater detail in the context of the hacking claim, his witness statement was misleading in relation to two significant matters. First, his witness statement implied that he did not produce written reports for the Ruler on his investigations whereas in fact he did so on a regular basis. Second, his witness statement said that he first came across the name of Mr Azima in early 2016 whereas in fact it was a year earlier. His evidence in connection with the discovery of the hacked material was both internally inconsistent and at odds with the contemporary documents. I have concluded that it would be unsafe to rely on any evidence from Mr Page that was not corroborated by some other source.
  
65. Amir Ali Handjani is on the board of RAK Petroleum and was involved in discussions with Mr Buchanan and Mr Bustami regarding both the money that Mr Azima said was owed to him and matters involving Dr Massaad. Mr Azima criticised him as an evasive witness giving further dishonest evidence. Mr Handjani was criticised for his contention that the Ruler's instruction to "go after" Mr Azima was in part prompted by a demand for payment of \$8 million by Mr Azima. I do not regard the evidence on this point to be so clear cut as to justify the inference that he gave deliberately false evidence on it.
  
66. Naser Al Bustami sits on the boards of a number of companies owned by the government of RAK and is one of the Ruler's advisers. He was criticised for an email proposing that the Government of Georgia be enlisted to support RAKIA's claims against Dr Massaad. It is not clear from the email what assistance Mr Bustami had in mind and his oral evidence was that the assistance sought would be subject to Dr Massaad being convicted in a fair trial in a court of law. Even accepting that the email was improper, I do not consider that it supports the inference that Mr Bustami was a dishonest witness.
  
67. Majdi Halabi gave evidence in relation to the discovery of the hacked material. As set out later in this judgment, I came to the conclusion that his evidence was inherently implausible and not credible.
  
68. Stuart Leach ran the specialist litigation division at the public relations agency Bell Pottinger at the relevant time. Dave King is the Chief Executive of Digitalis, an online reputation and digital risk management firm, who were engaged by Bell Pottinger. I consider that they were both reliable witnesses who were seeking to assist the court.

69. Nicholas del Rosso gave evidence as to his involvement in retaining NTi to download the Hacked Material from the BitTorrent sites. His evidence was uncontroversial.
70. For Mr Azima, there were three witnesses. First there was Mr Azima himself. Second there was Mr Adams, a close friend and confidant of Mr Azima who deals with the accounts and paperwork for Mr Azima's business, who provided a short witness statement expressing agreement with Mr Azima's first witness statement. Finally there was Professor Donald Fowler, a friend of Mr Azima, who did not appear at the trial but provided an unchallenged witness statement describing an assignment that he had carried out for the Ruler at Mr Azima's request.
71. Mr Azima is a businessman with more than forty years' experience in all aspects of aviation, the airline industry and logistics. He has served as chairman of various airlines in different parts of the world. I am told that he has never before faced an allegation of fraud. RAKIA submitted that Mr Azima and Mr Adams were dishonest witnesses. After hearing evidence from Mr Azima and Mr Adams, I reached the conclusion that their evidence in opposition to RAKIA's claims was frequently inconsistent with the contemporaneous documents and inherently implausible. One example was their evidence concerning the retrospective drafting of the Joint Venture Agreement, which I deal with at paragraphs 123 to 128 below. I consider that Mr Azima and Mr Adams, in giving evidence, were more concerned to support Mr Azima's case than to assist the court with an honest recollection of the true facts.
72. The two expert witnesses, in the field of Computer Forensics and Investigations, were Christopher Tarbell (for Mr Azima) who is Director of Cyber Security and Investigations in the New York office of BRG, a global consulting firm, and Winston Krone (for RAKIA), who is Global Managing director in the Amsterdam office of Kivu Consulting Inc, a global technology firm. The experts each produced an expert report and together a joint report. The parties agreed that the experts, between whom there was a large measure of agreement, would not be called to give oral evidence.

### **Documentary evidence**

73. Mr Azima made wide ranging criticisms of RAKIA's documentary evidence and invited me to draw inferences against RAKIA on the ground that it had destroyed relevant documents.
74. Mr Buchanan's disclosure statement referred to an incident at the Covent Garden Apple store on 16 October 2016 when a substantial number of emails had been inadvertently deleted from his iPhone by an Apple employee. In witness statements filed for the purposes of an interim application before HHJ McCahill QC, it was explained that Mr Buchanan had attended the Apple store because of a problem in sending emails from his phone. On 22 October 2016, six days later, Mr Buchanan was informed of the need to preserve documents, whereupon he informed Dechert of the possible deletion of emails. Steps were then taken to address the situation by restoring the deleted emails but these were only partially successful.
75. It was submitted for Mr Azima that it was "very likely" that Mr Buchanan deliberately

company. [...]

... [D]ue to the failure of RAK Airways to provide its share of the joint venture investment, the amount HeavyLift has already disbursed needs to be repaid."

- 129.2 Mr Stewart replied the same day explaining that he was "not familiar with the agreement" and asking, "when the agreement was originally signed". Mr Adams replied by attaching a copy of what he claimed was "a copy of the 2007 Joint Venture Agreement" which had been produced and signed the previous week.
- 129.3 On 2 October 2013, Mr Azima sent an email to the Ruler concerning the Training Academy JV. The email began: "I am not sure how to bring an unresolved business matter to your Highness as I never have before". This statement contradicts Mr Azima's claim that he spoke with the Ruler about the joint venture in 2010 and supports the Ruler's denial that any such conversation took place. The email made no reference to an alleged agreement with RAK Airways regarding the value of HeavyLift's investment in the Training Academy joint venture.
- 129.4 In June 2015 Mr Azima introduced Ms Azadeh to RAKIA to present his position on HeavyLift's claim for compensation. On 13 June 2015, Mr Buchanan met with Ms Azadeh and made it clear that RAKIA was willing to investigate HeavyLift's claim to ensure a fair outcome.
- 129.5 According to Mr Adams' witness statement, following that meeting, he was asked by Mr. Azima to provide additional information and documentation requested by Mr. Buchanan on behalf of RAKIA to assist them with quantifying the amount which they would be "reimbursing" HeavyLift for its involvement in the joint venture.
- 129.6 By an email sent on 14 June 2015, Mr Buchanan requested detailed information and records concerning the project including various "Financial records, asset register and reports". In particular, he requested amongst other things (a) "financial records that back up the Statement of Account and show all investments made by HeavyLift into or on behalf of the JV, including date, account details etc"; and (b) "details of the assets owned or held/used by the Training Academy JV to the extent not already forming part of the financial data". Mr Buchanan also asked: "More generally, what (if any) information can you provide about RAK's actual contribution [to] the joint venture in financial terms?".
- 129.7 On 6 July 2015, Ms Azadeh sent a letter from Mr Adams to Mr Buchanan which stated that prior to the termination of the Training Academy JV "HeavyLift had already invested \$2.5 million." The letter further stated that while hard copies of the Training Academy JV's audited accounts for 2007 and 2008 were not available, an extract from the "Director's Report and Balance Sheet Signature page" showed that as of 31 December 2008 the "Total Investment by

Adams to Jim Stewart. None of those involved in the original arrangements remain in RAK, and some of the RAK companies that appear to have been involved have been restructured”.

- (b) On 9 August 2015, Mr Buchanan sent an email to Ms Azadeh which explained that there were significant “difficulties in identifying and assessing information that might enable us to respond properly to the issues you have raised”. Given the difficulty in locating relevant records, Mr Buchanan therefore requested Ms Azadeh to “set out your claims against RAK Airways in greater detail and provide evidence to support those claims”.

147.4 Mr Azima’s assertions that the inducement requirement is not made out because RAKIA entered into the Settlement Agreement “for purposes unconnected to the settlement of the claim” and because it had reached an “internal evaluation...that Mr Azima was acting against RAKIA, and fraudulently” is incorrect.

147.5 If a misrepresentation is of such a nature that it would be likely to play a part in the decision of a reasonable person to enter into a transaction it will be presumed that it did so unless the representor satisfies the court to the contrary; *Dadourian v Simms* [2009] EWCA Civ 169.

148. Mr Azima denies that RAKIA has established reliance. He submits as follows:

148.1 The evidence at trial established that the decision to enter the Settlement Agreement was taken by the Ruler, not by Mr Buchanan or the board of RAK Dev or the board of RAKIA. Mr Buchanan’s evidence established that his function was to make a “recommendation” and the actual power to decide rested with the Ruler. His oral evidence confirmed clearly that entry into the Settlement Agreement was the Ruler’s personal decision:

“Q. And it's right, isn't it, that the decision to enter into the settlement agreement was taken on behalf of RAKIA by the Ruler? A. That is correct.  
Q. It wasn't taken by you, was it? A. That is correct.”

148.2 Mr Gerrard’s evidence was similarly that the Ruler was the “ultimate authority in RAK” and “if RAKIA was to undertake a course of events that he didn’t approve of” it “wouldn’t necessarily happen.”

148.3 Mr Buchanan also confirmed that he did not know the Ruler’s reasons for entering into the Settlement Agreement:

“Q. Thank you. You are not in a position, are you, Mr Buchanan, to give evidence as to what the Ruler may have -- what may have influenced the Ruler into entering into the settlement agreement in March 2016? A. No, I'm not.”

148.4 There is no evidence that the Ruler had regard to or relied on the alleged representation by Mr Azima as to the contribution made by HeavyLift into the Training Academy. Nor does the Ruler suggest that he relied on Mr

## Were the stories false?

201. Mr Azima submits that:

- 201.1 RAKIA failed to adduce any evidence in its witness statements that the stories said to have been procured and promoted by Mr Azima were in fact false;
- 201.2 RAKIA attempted to fill this gap through a series of leading questions to Mr Gerrard in re-examination in which Mr Gerrard denied that he had been involved in illegal detentions in RAK or had taken on prosecutorial or judicial roles. Mr Gerrard's answers, elucidated in this way at the end of his evidence, were simply not a sufficient basis for this Court to find that the "falsity" of any alleged media stories is established.
- 201.3 This is particularly so in circumstances where there was evidence showing that concern at detentions in RAK was well-founded, and there was also evidence of Mr Gerrard's and/or Dechert's role in those detentions giving rise to legitimate concerns. It was incumbent on RAKIA to address these issues with evidence, which it has not even attempted to do.
- 201.4 Mr Azima referred to a November 2014 Amnesty International report referring to several cases in which individuals had in fact been detained for long periods in the Ruler's palace or in other undisclosed locations. None of RAKIA's witnesses were in a position to refute its findings.
- 201.5 Reports had been provided to Mr Azima about Mr Gerrard conducting (on behalf of the Ruler and/or RAKIA) highly aggressive and unlawful interrogations of prisoners including Mr Al Sadeq; and aggressively threatening Mr Al Sadeq's wife and threatening one of RAKIA's opponents (Mr Izadpanah) with prison unless he agreed to pay \$7.5 million to RAK, and offering clemency in exchange.
- 201.6 Under cross-examination, Mr Gerrard accepted that he had in fact interviewed Mr Al Sadeq and other individuals while in prison in RAK. He also admitted investigating and interviewing Mr Izadpanah in RAK.
- 201.7 If RAKIA was to sustain its case that complaints about these practices in RAK were false, disclosure should have been given of these incidents including of the records of interview that Mr Gerrard said would exist. This is particularly so given that Mr Gerrard's own account of Mr Al Sadeq's interview in detention itself raised concerns. Mr Gerrard claimed that the interview had been conducted strictly pursuant to the standards in the Police and Criminal Evidence Act 1984 although it became clear in Mr Gerrard's evidence that this was not true. No audio recording of the interview was made and he was unsure whether a record of the interview had been provided to Mr Al Sadeq's lawyers. Mr Al Sadeq was detained in RAK without charge for at least a year. Mr Gerrard accepted that he interviewed Mr Al Sadeq at some point during that detention, before he was charged.

201.8 Mr Gerrard saw no problem with an individual being detained for a prolonged period without charge and being interrogated in that period: “They have a process. It is not like ours -- many parts of it are -- and he agreed to talk to us whilst he was detained. We followed the process of PACE when we met him.” As noted, the claim that PACE was followed was not correct, on Mr Gerrard’s own evidence.

## Conclusion

202. In order to make good its case that Mr Azima procured and promoted false stories in the media, it was incumbent on RAKIA to establish that the stories which it was intended to publish about human rights violations were untrue. It has not done so. It appears that Project Clay intended to draw attention to actual cases of detention and illegality, not fabricated cases. The 2014 Amnesty International Report indicates that there were real grounds for concern about detention procedures in RAK. None of RAKIA’s witnesses were in a position to refute the findings in that report.

## Mr Azima’s role in relation to the Security Assessment

203. The facts relating to the Security Assessment as they appear from the documents before the Court were as follows:

- 203.1 In late 2014 Mr Azima was engaged by Mr Kirby Behre, a lawyer at Miller & Chevalier, lawyers who acted for Dr Massaad (and later Mr Azima) to act as a consultant to assist with a PR campaign involving the investigation of human rights abuses in RAK for the benefit of Dr Massaad who had fled RAK and was in dispute with RAKIA and the government of RAK.
- 203.2 Mr Azima introduced former CIA operative Scott Modell to Dr Massaad and Miller & Chevalier and commissioned him to produce the Security Assessment and was responsible for arranging Mr Modell’s remuneration for producing it.
- 203.3 The Security Assessment consisted of a review of the security issues affecting Dr Massaad including a detailed series of “Recommendations” which included “aggressive tools” and “offensive media operations” to “display the critical weak points of the RAK”, using media teams to “denigrate the reputation of Sheikh Saud and the RAK as a place of doing business”, and a campaign going beyond negative stories and including: “Organized protests and other forms of manufactured dissent, sustained over an extended period of time”.
- 203.4 The Security Assessment also included a recommendation for “orchestrating business deals in RAK with disreputable individuals from other parts of the world” setting out how the RAK Government, the ruling family and RAK-owned banks and businesses could be deceptively lured into entering

255. Mr Azima's pleaded case in support of his hacking claim (at paragraph 8J of the Re-Re-Amended Defence and Counterclaim) is as follows.

- “(a) Between autumn 2015 and July 2016 Mr Azima was assisting in the mediation of a dispute between RAKIA and Dr Massaad.
- (b) To the best of Mr Azima’s knowledge, on or around 14 October 2015 Mr Azima received several emails containing malicious internet links which were aimed at him specifically so as to induce him to open the emails. The opening of the emails and the links in them enabled those carrying out the hacking to gain unauthorised access to and steal Mr Azima’s confidential data.
- (c) RAKIA has targeted Mr Azima in the context of its dispute with Dr Massaad. In particular, in around April 2015, the Ruler told Mr Buchanan that he wanted Mr Buchanan and other assistants to "target" Mr Azima. The Ruler directed his associates to bring "charges" against Mr Azima and also to pursue "other channels" for taking action against Mr Azima. The Ruler's associates discussed meeting to "coordinate our attack" on Mr Azima and Dr Massaad. In or around July 2015, the Ruler instructed another of his assistants, Mr Bustami, to "go after" Mr Azima. Further, in the context of his role in assisting in the mediation of the dispute between RAKIA and Dr Massaad, Mr Azima had meetings and discussions with RAKIA's representative, Mr Buchanan, and its counsel, Mr Neil Gerrard, of Dechert LLP. At a meeting on or about 23 July 2016, Mr Gerrard told Mr Azima that if Dr Massaad would not agree to a settlement, Mr Azima would be made "collateral damage" in a war that RAKIA would then wage on Dr Massaad. Mr Azima understood this statement to be a threat.
- (d) The dispute between RAKIA and Dr Massaad was not resolved. RAKIA engaged investigators and public relations consultants (including the now defunct firm, Bell Pottinger) to make inquiries into Mr Azima and to disseminate information about him.
- (e) On around 29 July 2016, Mr Azima learned of a website making allegations against Dr Massaad, similar to those which RAKIA had made in the course of the mediation of its dispute with Dr Massaad. Shortly thereafter, Mr Azima learned of two other websites containing similar allegations against him. The websites contained links to BitTorrent internet sites, where certain materials stolen from Mr Azima were available to download with appropriate software and expertise. At this point, Mr Azima apprehended that his emails and data had been stolen, and so changed his passwords and increased his computer security.
- (f) RAKIA has admitted that it and its lawyers, Dechert LLP, hold a substantial quantity of the data stolen from Mr Azima, including an admission made in September 2016 to holding around 30GB of material. RAKIA denies responsibility for the hacking and theft of data or awareness of the persons responsible. Its explanation for holding these materials, given through its solicitor Mr David Hughes, is that the materials were obtained from internet sites. In proceedings brought by Mr Azima against RAKIA in the United States

257.5 RAKIA was able to gather information about Mr Azima from the hacked material by December 2015, as evidenced by the View from the Window document;

257.6 Although Mr Azima had (on his case) a genuine entitlement to receive \$2.6 million in compensation from RAKIA in respect of the Training Academy JV, the Settlement Agreement was in fact a device which was intended to equip RAKIA with a legal mechanism to bring a claim against Mr Azima on the basis of material which it already had from hacking his emails. The \$2.6 million was paid to “lure” Mr Azima into an agreement, to “reel him in and use him in our negotiation with Dr Massaad”.

257.7 RAKIA’s case as to how it came across the hacked material innocently was untrue and designed to conceal RAKIA’s role in the hacking. Contemporaneous emails which show that RAKIA innocently discovered the hacked material were in fact a false “paper trail” created by Mr Buchanan and Mr Gerrard in order to conceal their involvement in the hacking.

257.8 Wrongdoing can be inferred from RAKIA’s “highly suspicious” approach to the documentary evidence.

258. RAKIA’s position is, in summary, as follows.

258.1 The hacking claim is unfounded. RAKIA had no involvement whatever in the hacking of Mr Azima’s emails/devices or in the publication of any hacked documents online. These were documents which were publicly available on the internet which were discovered by individuals who reported them to RAKIA in early August 2016 at about the same time as the documents were discovered by individuals acting on behalf of Mr Azima.

258.2 An allegation that a party engaged in a criminal conspiracy to unlawfully hack into and publish a person’s confidential data in pursuit of a malicious vendetta, and then took extensive steps to deliberately and dishonestly conceal that criminal activity from the Court, is an allegation of the utmost seriousness. It is trite law that cogent evidence is required to justify a finding of discreditable conduct and that “the cogency of the evidence relied upon must be commensurate with the seriousness of the conduct alleged”.

258.3 These principles required Mr Azima to adduce particularly cogent and persuasive evidence in order to make good his hacking claim. Mr Azima’s hacking claim necessarily entails not only a claim that RAKIA dishonestly obtained access to his emails but that its witnesses including Mr Buchanan, the Ruler, Mr Gerrard, Mr Halabi, Mr Bustami and Mr Handjani were parties to a conspiracy to deceive the court by the presentation of a fundamentally false case concerning RAKIA’s role in the hacking of Mr Azima’s emails.

258.4 In any event, whatever the position about RAKIA’s direct or indirect involvement in hacking, the public interest in the fair and just disposal of the

following the Project Update, the Ruler was concerned about Mr Azima and interested in pursuing him. The Ruler said in his witness statement that in early 2015 he wanted information about Dr Massaad's organised criminal scheme and, in particular, as to the role Mr Azima had played. It seems most unlikely that he did not discuss Mr Azima with Mr Page, the investigator with whom he was having monthly meetings, in which case it is hard to believe that Mr Page could have completely forgotten about any mention of Mr Azima prior to his meeting with Mr Buchanan in early 2016.

**(2) The April and July 2015 emails**

279. On 4 April 2015, Mr Buchanan emailed Mr Handjani as follows:
- “HHSS [i.e. the Ruler] had wanted us to target FA [i.e. Mr Azima] – on what basis would we do this?”
280. It is unclear precisely what prompted this email. Mr Handjani’s evidence, which I accept, was that Mr Azima had called him out of the blue in March 2015 and said that there was a big problem between him and the Ruler in that he was owed \$8m by RAK and that, if things were not resolved, they could “get ugly” for everyone. Mr Handjani was also called by Dr Massaad at about this time who asked him to talk to the Ruler and get the Ruler to stop investigating him. Mr Handjani then spoke to the Ruler about both calls.
281. Mr Buchanan’s evidence was that the Ruler’s instruction to target Mr Azima in April 2015 was prompted in part by Mr Azima’s claim for \$8 million, which the Ruler considered to be unfounded, and in part by the information in the Project Update. He said that the reference to “targeting” was a reference to the bringing of criminal charges.
282. The Ruler’s own evidence as to his state of mind was that he wanted information about the extent of the criminal scheme organised by Dr Massaad and, in particular, as to the role Mr Azima had played and, if he was involved in those schemes, to have criminal charges brought against him. He dismissed the suggestion that the emails were prompted by the Project Update.
283. The email of 4 April 2015 led to the following exchanges on the same day:
- (a) Mr Handjani: “I’m not sure that’s possible at the moment. I don’t know what basis you would target him. Thoughts?”.
  - (b) Mr Bustami: “As for Farhad, I would say get AH [Mr Handjani] on the case to check with the boss on what exactly he wants done”.
  - (c) Mr Buchanan: “AH has no idea how we might go after him”
  - (d) Mr Bustami: “I think next week Amir is in town so we can both hook up with him and brain storm it.”
284. Later that day, Mr Bustami wrote to Mr Handjani and Mr Buchanan as follows:

"I have had few discussions with boss about FA [Mr Azima] and he is adamant that we bring charges against him. He was very happy that you told him that FA is no longer asking for the \$8 m.

The boss told me that you have checked with your people and confirmed back to him that the boys with the hotel are no issue now and we should not be intimidated by them and that FA may not be orchestrating this.

He wants me to get you on the case to file some sort of charges against Farhad. He also told me today that you have another channel that you are using with khater [Dr Massaad]. When are you next in town so that me you and Jamie [Mr Buchanan] could hook up and coordinate our attack?"

285. Mr Handjani's evidence, which I accept, was that the reference to "going through another channel" was a reference to attempts that were going on at that time to open a dialogue with Dr Massaad.

286. On 6 April 2015 Mr Handjani wrote to Mr Bustami and Mr Buchanan as follows:

"Subject: Re Farhad Azima

Dear Naser

Thank you for your email. I spoke to the boss and advised him against both using other channels and pressing charges against Farhad for now. I believe both approaches could undermine the work that you and Jamie are doing. I was very clear with him that we should speak with one voice-and for the moment you and Jamie are that voice.

We have to see how Khatter responds with his lawyer. If we start pressing charges with Farhad it would disrupt this process. My humble opinion is that we should not be fighting multiple fires at one time.

We need to keep this circle of information tight and give full weight and support to you and Jamie.

I have advised boss as much as  
well. Best,  
AAH"

287. There is no evidence of any steps being taken against Mr Azima between April and July 2015 and the natural inference from this email is that the Ruler was dissuaded from taking any action for the time being. Mr Buchanan's evidence was that Mr Azima did not feature at all in his discussions with the Ruler in this period.

"Q. What was going on in relation to investigating Mr Azima between the beginning of April 2015 and 19 July 2015?

A. Absolutely nothing to my knowledge.

Q. Did you have some monthly meetings with Mr Page over this time?

A. Yes, I would have done.

Q. And would there have been some reports in all likelihood, written reports?

A. Yes, written or verbal, and I can't tell you which they were.

Q. And you would have discussed those with the Ruler?

A. I would have done -- I did.

Q. And is it your evidence that Mr Azima didn't feature at all in any further updates from Mr Page between the beginning of April 2015 and 19 July 2015?

A. I have no recollection of Mr Azima's name or his activities coming on to the radar screen in that period."

288. On 19 July 2015, Mr Buchanan wrote to Mr Handjani as follows:

"NB [Naser Bustami] says the Boss wants criminal stuff taken out of letter and to go after FA subject to guidance from AF [Andrew Frank].

Nothing ELSE new from NB - will speak to AF tomorrow and fill you in."

Mr Handjani replied as follows:

"Talking to the boss now. He wants me to respond to the little guy in an email and to coordinate with you."

289. Mr Buchanan's evidence about this exchange in his witness statement was that he had received a message from Mr Bustami to the effect that the Ruler wanted criminal allegations taken out of a letter to be sent to Dr Massaad's lawyers. The reference "to go after FA" was a reference to the prospect of some form of criminal proceedings or criminal charges being brought against Mr Azima which were not in the event pursued although in cross-examination, Mr Buchanan said that he did not know what was meant by "going after FA". "Guidance from AF" was a reference to guidance being sought from Mr Andrew Frank who provided public relations assistance to RAK in the US and whose guidance would be sought in relation to any reputational issues that might arise as a result of criminal charges being brought against Mr Azima as a US citizen. The reference to "the little guy" was a reference to Mr Azima. Mr Buchanan said that the planned coordinating was to do with the HeavyLift claim for compensation about which Mr Azima had emailed Mr Handjani on the same day (19 July 2015). Mr Bustami's and Mr Handjani's evidence was to the same effect. On 28 July 2015 Mr Handjani sent a response to Mr Azima explaining that there was nothing he could do beyond putting him in touch with Mr Buchanan.

290. It is unclear what prompted the Ruler to give the indication or instruction reflected in Mr Buchanan's email of 19 July. Mr Buchanan was unable to explain what prompted the Ruler to want Mr Azima to be "gone after" at this time. What is clear is that the Ruler's desire for action to be taken against Mr Azima had not abated since April. The evidence of Mr Buchanan and Mr Handjani was that this desire was prompted in part by annoyance over what the Ruler perceived was an unmeritorious claim for the \$8 million but this seems unlikely given that Mr Handjani's email of 4 April 2015 had made clear that this claim was not being pursued. The Ruler himself does not suggest that the \$8 million claim prompted his desire to go after Mr Azima. It is more likely that the Ruler's hostility towards Mr Azima stemmed from his perception, originating in the Project Update, that Mr Azima was an associate of Dr Massaad who was threatening to cause trouble for him.

countries with which Mr Azima had no connection. Mr Krone accepts that this access appears to be suspicious.

300. In summary, it is possible that the hacking of Mr Azima's emails is linked to his receipt of spear-phishing emails in October 2015 but this is not firmly corroborated by the evidence. There is no evidence as to who carried out the hacking.

#### **(4) The View from the Window document**

301. Following the alleged hacking in October/November 2015, on 29 December 2015 a document was prepared on RAKIA's side which described a "series of investigations" and labelled Mr Azima as a participant in "fraudulent activities". It was prepared by Andrew Frank, a senior individual at Karv Communications, a PR company working for RAKIA, who had been mentioned in Mr Buchanan's email of 19 July 2015. It was sent to Mr Gerrard on 4 January 2016.

302. The document reads as follows:

**"View from the window**

The window has opened on Ras Al Khaimah through a series of investigations that have unearthed a massive fraud that has taken place in the Emirate, the UAE, and several other countries including the Republic of Georgia, India, Congo and others.

A number of things have been exposed as fact over the past twenty-four months:  
-KM was the CEO of RAK Ceramics beginning in 2003, as well as the RK Investment Authority (RAKIA) beginning in 2006 and oversaw a series of investments inside and outside of RAK that are under now intense scrutiny and have exposed wrong-doing

-Gila Mikadze was head of RAKIA's operations in Georgia and created and oversaw numerous corporations that stole money from the Emirate and was used for his own purposes and to bribe former government officials.

-Others committed crimes inside RAK, including the Ruler's Chief legal advisor and the legal advisor to RAKIA (they also happen to be cousins(?))

... -FA, a U.S. citizen, appears to have orchestrated, if not (fully) participated in numerous fraudulent activities.

... -Companies were set up with Iranian nationals"

303. Mr Azima's case is that the reference in the document to "FA" (i.e. Mr Azima) appearing "to have orchestrated, if not (fully) participated in numerous fraudulent activities" establishes that RAKIA must by this stage have hacked into Mr Azima's emails because otherwise Mr Frank would not have known about what RAKIA alleges in these proceedings to be his "fraudulent activities".

304. In support of this case, Mr Azima submits as follows:

- 304.1 It is striking that none of RAKIA's witnesses even acknowledged the existence of the View from the Window document. RAKIA failed to call Mr Frank

as a witness and failed to identify Karv when ordered by HHJ Kramer QC to identify its public relations consultants, indicating an awareness that his evidence would be damaging to RAKIA.

304.2 The View from the Window document establishes “beyond serious argument” that by the end of December 2015, RAK and RAKIA had obtained access to Mr Azima’s confidential emails and data. The author of the document had clearly been informed that RAK and RAKIA had a firm basis for asserting that Mr Azima had orchestrated or participated in “numerous fraudulent activities”.

304.3 A belief on RAKIA’s part that there was such a basis could only have come from the hacked material. As Mr Buchanan, who was leading RAKIA’s investigation, explained, RAKIA only believed that Mr Azima had engaged in any fraud upon reviewing the Hacked Material:

“A. The investigations that had taken place until that point gave me no cause to believe that Mr Azima was involved in any frauds in respect of Dr Massaad.

Q. But you changed your mind when you saw the hacked data; is that right?

A. I changed my mind when I saw the hacked data, that is correct.”

304.4 When Mr Buchanan was shown the View from the Window document, he claimed to be able to offer no explanation for its contents and to have been unaware of it until it was put to him in cross-examination.

304.5 Mr Gerrard gave inconsistent explanations for the document, alleging initially that it was “ramblings” of Mr Frank which had come “out of the blue” and later that it was the product of a meeting which had taken place two weeks earlier concerning a “blitzkrieg” of negative publicity. He claimed that he told Mr Frank that the section of the View from the Window concerning Mr Azima “isn’t going to work” because all that was known about Mr Azima was “suspicious”.

304.6 This account is not credible given the absence of any response by Mr Gerrard to Mr Frank’s email attaching the View from the Window document and the inconsistency with the evidence of Mr Buchanan, according to whom the “blitzkrieg” meeting did not take place until January 2016. Moreover, the View from the Window does not purport to describe “suspicious”. It states that investigations have “unearthed a massive fraud” and that the matters listed in it (including Mr Azima’s involvement in “numerous frauds” “have been established as fact”.

305. The View from the Window document shows that in late 2015, a negative PR campaign was being planned against Mr Azima alongside Dr Massaad. Mr Azima had not dropped out of the picture. It also suggests that someone had planted in Mr Frank’s mind the idea that Mr Azima had been involved in fraudulent activities. That

person was probably Mr Gerrard who had briefed Mr Frank before the document was sent. It was put to Mr Gerrard in cross-examination that, in order to have accused Mr Azima of fraud, Mr Gerrard must have been aware of the contents of Mr Azima's confidential emails:

"Q. ... by that stage, I suggest, Mr Gerrard, you were aware of the confidential material that had been procured illegally from within Mr Azima's email records in October/November 2015 and one way or another you thought you were on to something. You started to think that you could -- that you had some material to allege fraud. That's what I put to you.

A. So I'd like to deny that, my Lord. It's preposterous. But I'd also like to explore that question because what you're suggesting is I had a secret little stash of Mr Azima's documents which I could select at will to identify frauds. I mean, how would I do that? How do I pull this stuff down? How do I search for it?"

306. Shortly thereafter, the following exchange took place:

"Q. And you would have been aware that Mr Page had been successful in gathering intelligence from within Mr Azima's confidential email archive?

...

Q. I'm putting that to you.

A. Right. No, I wasn't aware.

Q. And that this is the only explanation for why Mr Frank has recorded, based upon what you and Mr Buchanan must have told him, the idea that Mr Azima had been involved in numerous fraudulent activities.

A. My Lord, that's ridiculous. Mr Frank is a clever man, but he's not a lawyer. He will have heard on a regular basis concerns as to gun-running, fraud, etc, etc. What he will not have grasped that we did not have sufficient evidence to proceed. On everything else we had stacks of evidence against -- let's take the first bullet point, Dr Massaad. We had evidence. Indeed he was prosecuted. We had evidence against Mikadze. He was prosecuted. We had evidence of other crimes inside RAK, including the Ruler's chief adviser and the general counsel. They were prosecuted. Let me ditch Farhad Azima for the moment. We had dummy corporations set up in the RAK, UK, Georgia, Cayman Islands, etc. We could have put those in, and so on. Fraudulent bank accounts, possible gun-running ... we did not have any evidence that we could have proceeded against of actual fraud against Farhad Azima. That is just plainly wrong and that's what I told Andrew Frank"

307. Mr Gerrard's explanation for the reference in the View from the Window document to Mr Azima's "orchestrating if not participating" in "numerous fraudulent activities" was confused. At one point he referred to the Project Update, although this had not alleged fraud against Mr Azima. He also referred to information provided to Mr Frank at a meeting attended by Mr Buchanan, although this meeting did not take place until later. His evidence was essentially that Mr Frank was told about suspicions concerning Mr Azima but these suspicions had nothing to do with Mr Azima's hacked emails.

document destruction, much less of any instruction by RAKIA to destroy relevant documents.

**(7) The July 2016 meeting**

322. Following execution of the Settlement Agreement in March 2016, Mr Azima continued to engage with RAKIA with a view to brokering a settlement of its dispute with Dr Massaad.
323. On 16 July 2016, a meeting was held between Mr Azima and three representatives of RAKIA: Mr Buchanan, Mr Gerrard, and an associate in Mr Gerrard's firm, Dechert, at the Churchill Hotel in London.
324. Mr Azima's case is that at this meeting Mr Gerrard threatened him that if Dr Massaad would not agree to a settlement, Mr Azima would be made "collateral damage" in a war that RAKIA would then wage on Dr Massaad, a threat that was put into effect a few weeks later.
325. Mr Azima's evidence was as follows:
  - 325.1 Mr Gerrard told him to stop acting as a mediator, and instead work solely for RAKIA to assist them in their campaign against Dr Massaad.
  - 325.2 He refused and told Mr Gerrard that is not how he operated; this aggravated Mr Gerrard who proceeded to reference his history, stating that he had been a policeman, a detective, a prosecutor and a lawyer, and that he had connections with "Number 10" and that if Mr Azima did not settle the case with Dr Massaad then there would be a war against Dr Massaad and Mr Azima would be "collateral damage".
  - 325.3 Mr Azima asked Mr Gerrard whether he was threatening him. He told Mr Azima that this was not a "threat but a promise."
  - 325.4 At the end of the meeting, he asked Mr Buchanan for a copy of the handwritten notes that Mr Gerrard's colleague had taken. Mr Buchanan informed Mr Azima that he would be sent a copy of the notes after they were transcribed that evening. However, after repeated chasing, Mr Buchanan said that Mr Azima could not have them without Mr Gerrard's permission. He also set out in an email dated 23 July 2016, in response to Mr Azima's complaint that what Mr Gerrard had said to him amounted to "extortion" and "blackmail", a dictionary definition of those terms.
326. Dechert's note of the relevant part of the meeting reads as follows:

"NG noted that Kirby had referred to "mutually assured destruction" but that KM was delusional if he thought that bringing the criminal and civil actions would destroy HHSS. NG noted that HHSS was now engaging with Abu

included email communications up to August 2016 suggesting that the hackers had access to Mr Azima's email accounts throughout the period from October 2015 to August 2016.

339. Mr Azima contends that the proximity in time between (i) the breakdown in the negotiations with Dr Massaad and RAKIA and the consequential appearance of the websites attacking Dr Massaad (which RAKIA admits to arranging through Digitalis) and (ii) the websites with links to the hacked material, cannot realistically be a coincidence but is a clear indication that the Ruler or RAKIA were behind both attacks.
340. RAKIA contends that there is no connection between the Massaad websites and the appearance of the blogging websites with links to the hacked material and that it is inherently unlikely that sophisticated hackers (which is what the hackers would be, if Mr Azima's hacking claim were correct) acting on the instructions of RAKIA or the Ruler, would put up the blogging websites so soon after the Massaad websites as this would inevitably give rise to suspicion that both the blog websites and the Massaad websites were part of the same PR campaign and hence that RAKIA had carried out the hacking. On Mr Azima's case, RAKIA had had access to the hacked material since the preceding October 2015 and could have delayed publicising it for several more weeks or months. Mr Azima's answer to this point is that RAKIA may have been sufficiently confident that it had covered its tracks for it not to be concerned about detection.
341. In my judgment, if the hackers were acting on the instructions of the Ruler or RAKIA, it is unlikely that they would have timed the publication of the hacked material to coincide with the end of the "ceasefire" and the posting of the anti-Dr Massaad websites. It is more probable in my view that the two incidents, while close in time, were not in fact related. The posting of the Massaad websites was a deliberate PR campaign instructed by the RAKIA; the other was the unrelated act of hackers.

## **(9) RAKIA's alleged discovery of the hacked material**

342. RAKIA has sought to explain how it became aware of the hacked material on the internet. Mr Azima submits that RAKIA's account is false and dishonest and is advanced by RAKIA in order to cover up its own responsibility for the hacking.
343. RAKIA's pleaded case, and the case it advanced in its witness statements concerning its discovery of the hacked material, is, in summary, as follows:
  - 343.1 Following a meeting in January 2016 with Mr Azima, Mr Buchanan was alarmed by a warning from Mr Azima that, if RAKIA did not resolve matters with Dr Massaad soon, there would be an aggressive and negative public relations campaign directed against the individuals and companies involved and the Emirate of RAK more generally.
  - 343.2 Mr Buchanan discussed this warning with Dechert. It was decided that it would be prudent to take steps on RAK's behalf to prepare for any such

campaign, including by actively monitoring what was being published online. As part of that preparation, Mr Buchanan discussed Mr Azima's warning with various advisers including Mr Page.

- 343.3 In around February/March 2016, Mr Buchanan met with Mr Page and asked him to look out for anything relevant about a possible negative publicity campaign against RAK. Following that meeting, Mr Page contacted Mr Halabi and asked him to keep an eye out for anything interesting and unusual relating to RAK, the Ruler, Dr Massaad and Mr Azima.
- 343.4 Following Mr Page's request, Mr Halabi carried out Google searches for those names from time to time. During one of those regular Google searches in early August 2016, Mr Halabi discovered the blog sites containing links to a torrent file containing information relating to Mr Azima.
- 343.5 Mr Halabi therefore contacted Mr Page and sent him the links to the torrent sites. Mr Page then informed Mr Buchanan and Mr Gerrard about the links.
- 343.6 Mr Gerrard, in turn, contacted Mr del Rosso at Vital Management Services ("VMS") to seek advice on instructing a suitably qualified company to download the materials. Mr del Rosso emailed Chris Swecker, a former Assistant Director of the FBI and VMS's attorney, to ask for recommendations.
- 343.7 On Mr Swecker's recommendation, VMS then contacted Mr Garcia at NTi and engaged NTi to download the materials and to identify any other websites containing information relevant to Mr Azima.
- 343.8 On 23 and 24 August 2016, Ms Gray, a senior analyst with NTi, downloaded the contents of the files listed in the torrent file entitled "Farhad Azima of the Aviation Leasing Group Exposed" using BitTorrent software (the "First Tranche of the Internet Data").
- 343.9 On 1 September 2016, Mr del Rosso sent an email to Mr Swecker, Mr Garcia and Ms Gray informing them that a new dump of data relating to Mr Azima had been discovered online. The following day Mr del Rosso sent a further email with links to the torrent site. When she returned to the office the following week, Ms Gray downloaded the contents of the files that were listed in that torrent file (the "Second Tranche of the Internet Data").
- 343.10 Ms Gray thereafter continued actively searching for any additional information relating to Mr Azima. During the course of those searches on 9 September 2016 she discovered an additional dump of data relating to Mr Azima. She then proceeded to download the contents of the files listed in that torrent file (the "Third Tranche of the Internet Data").

343.11 NTi provided copies of the First, Second and Third Tranches of the Internet Data to Mr del Rosso. Mr del Rosso then provided those copies to RAKIA's lawyers at Dechert.

344. Mr Page deals in his witness statement with Mr Halabi's involvement as follows:

- 344.1 Following a conversation with Mr Buchanan in early 2016 in which he had been asked to keep his ears and eyes open for anything he heard about a negative publicity campaign that might be damaging for RAK, Mr Page spoke to a few contacts he uses occasionally in the investigations business, journalism and PR industry and asked them to keep their ear to the ground. One of those was Mr Halabi, whom he believes he met at a round table lunch in 2012. Mr Halabi is an Israeli journalist who specialises in Middle Eastern affairs. They have more of a friendship than a professional relationship.
- 344.2 At some point later that year, Mr Halabi called him and told him that he had come across something interesting on the internet about Mr Azima. As far as he could recall Mr Halabi sent him the website address where the material could be found in a WhatsApp message. He cannot check because he regularly deletes his WhatsApp messages for security reasons. Mr Halabi also told him that he believed the information came from the UAE. Mr Page did not ask why he thought this.
- 344.3 When Mr Page received this information from Mr Halabi, he would have picked up the phone to Mr Buchanan although he does not specifically remember doing so. He believes that Mr Buchanan asked him then to contact Neil Gerrard at Dechert and let him know what he had heard but it may have been the other way round.
- 344.4 A few weeks later, he learned that a second set of data relating to Mr Azima had been put onto the Internet. He cannot recall when or how exactly he learned of this. As he had not discussed the first set with any of his sources other than Mr Halabi, he believes it may have been Mr Halabi that told him about the second set but it is possible that he was told by one of his other sources. He does not recall being told anything about how or when the second set had been discovered. He believes that he would have called Mr Buchanan or Mr Gerrard immediately. He made no attempt to download the data.
- 344.5 He was never asked to hack or otherwise access Mr Azima's emails or data by RAKIA or anyone else. He does not know who hacked Mr Azima's computers or placed his data online. His involvement in this matter was limited to passing on of information provided by sources to RAKIA.

345. Mr Page's evidence in cross-examination was different from his witness statement in that he claimed that he passed on the information that he had received from Mr Halabi on a single occasion and that was the end of his involvement.

Halabi to Mr Gerrard and Mr Buchanan on or around 8 or 9 August 2016, he considered the task complete and did not contact Mr Gerrard or Mr Buchanan again. Mr Halabi was also clear that he only spoke to Mr Page on one occasion.

- 349.8 There is therefore no explanation in the evidence as to how RAKIA found out about the Second Tranche of Data.
350. There are further discrepancies between the evidence of Mr Page and the documents. On 16 August 2016 Mr Buchanan emailed Mr Frank and Mr Handjani, copied to Mr Gerrard, as follows.

“Good morning. I have been informed by Stuart last night that there is an internet site that is carrying a huge amount of material relating to FA - I will get you the link later. I have asked Neil to have a team start reviewing the material as a matter of urgency. At this time, I have no idea whether this relates to us or whether it is of value in respect of our ongoing dispute with KM. More importantly, I cannot tell you whether there is anything on the site about which we should have any concern. Clearly, it would be very interesting to know who is behind this action - Stuart tells me it is UAE based. We will speak later. Jamie”

351. This email raises further questions.
- 351.1 The email reads as Mr Buchanan was “breaking the news” regarding the hacked material (as Mr Buchanan accepted in cross-examination) even though, on RAKIA’s case, Mr Buchanan had been informed of the Hacked Material by Mr Page over a week before, on 8 or 9 August 2016.
- 351.2 Mr Page denies contacting either Mr Gerrard or Mr Buchanan after the initial alleged call in which he passed on the two links from Mr Halabi, which is said to have taken place on 8 or 9 August 2016. It follows that Mr Page did not contact Mr Buchanan on 15 August 2016.
- 351.3 Mr Buchanan’s email states that he would “get the link later”. There is no evidence that Mr Buchanan ever did get “the link” or that any of the recipients of the email followed up to ask for the link. Mr Gerrard’s evidence is that he believed that he “already had it by then” but there is no evidence that Mr Gerrard was provided with a link on 15 August 2016 or that he provided a link to anyone else at that time or thereafter. The emails between Mr del Rosso and NTi do not identify any such new link being provided.
- 351.4 No reply was sent to this email at all, by any of the recipients despite the dramatic nature of the news that Mr Buchanan had ‘broken’.
- 351.5 The email refers to “Stuart”, meaning that Mr Buchanan understood his audience – Mr Frank and Mr Handjani – to know who Mr Page was and that he was undertaking some sort of work for RAKIA.

is not true and that the true facts as to how RAKIA came to know about the hacked material have not been disclosed.

356. It does not of course necessarily follow from this conclusion that RAKIA was responsible for the hacking. As RAKIA pointed out, there would be variety of explanations for Mr Page's failure to give a true account of the discovery. He may, for example, have wanted to conceal his sources of information, even though they were not the hackers, for reasons of confidentiality.

**(10) RAKIA's deployment of the hacked data**

357. Mr Azima submits that RAKIA's responsibility for the hacking should be inferred from the fact that, apart from RAKIA no other party in any jurisdiction has sought to use any of Mr Azima's stolen material in any proceedings or indicated that it was able to access the stolen data using the BitTorrent sites.

358. RAKIA's response to that argument is that Mr Azima appears to have been the subject of long term interest by Iran who perceived him as an enemy of the Iranian Government and who actively sought to acquire information and intelligence about him by targeting his communications and the communications of his close associates. In particular:

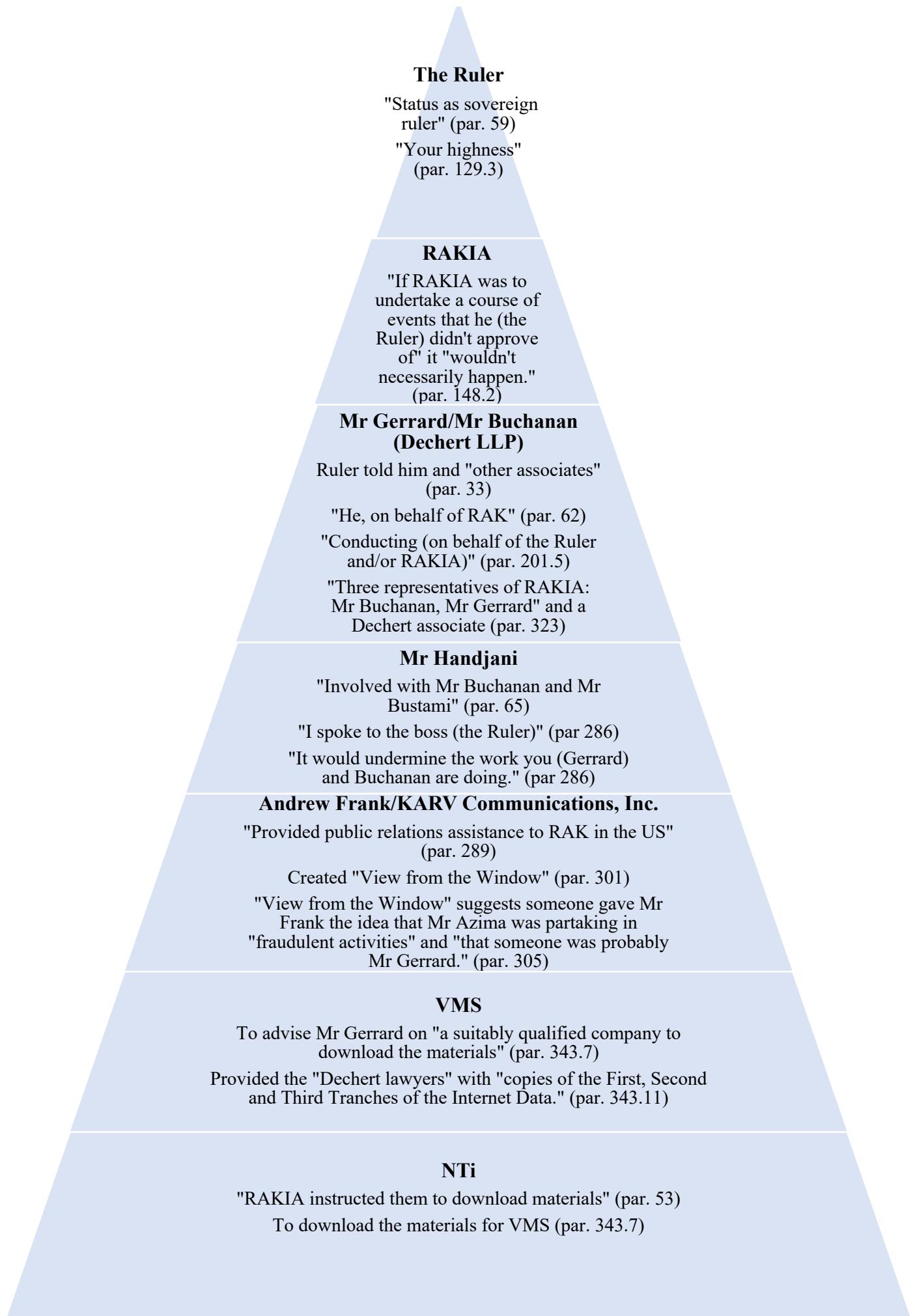
358.1 On 2 September 2012, for example, Ms Azadeh sent an email to Mr Azima which described how Mr Azima was being spied on by agents of Iran. The email was sent after Ms Azadeh was arrested and detained for more than three months by the Iranian Government and Revolutionary Guards.

358.2 On 24 February 2016, Ms Azadeh emailed Mr Azima a detailed account of her arrest and detention in Iran which made it clear that she and her communications were deliberately targeted by the Iranian state because of her close connection to Mr Azima, whom the Iranians believed was working with the CIA. She went on to explain that, "They had access to my computer and emails" and that she was eventually released after being "made to confess that I was a CIA agent and I was working with Farhad Azima in relation to all anti-Islamic government activities supported by U.S."

358.3 Jay Solomon, a former journalist for the Wall Street Journal, published an article in the Columbia Journalism Review dated 7 March 2018 which stated his belief that the Government of Iran was responsible for the hacking of Mr Azima's emails. The article recounted how emails between him and Mr Azima were hacked and put on the web as a torrent file. This happened just weeks after his first story broke in August 2016 about the Obama administration's secret cash shipments to Iran.

358.4 On 18 July 2016 – two weeks before the First Tranche of the Internet Data was published online – Ms Azadeh filed a lawsuit against the Islamic Republic of Iran and the Islamic Revolutionary Guards Corps before the United States

## PLAINTIFF'S EXHIBIT 2



## PLAINTIFF'S EXHIBIT 3

BRYAN SCHRODER  
United States Attorney  
JONAS M WALKER  
STEVEN SKROCKI  
Assistant U.S. Attorneys  
Federal Building & U.S. Courthouse  
222 W. 7<sup>th</sup> Avenue, #9, Room 253  
Anchorage, AK 99513-7567  
Phone: (907) 271-5071  
Fax: (907) 271-6011  
E-mail: jonas.walker@usdoj.gov

DEBORAH L. CONNOR  
Chief, Money Laundering and Asset Recovery Section (MLARS)  
WOO S. LEE  
Deputy Chief, International Unit  
MICHAEL OLMSTED  
Senior Trial Attorney, International Unit  
Criminal Division  
United States Department of Justice  
1400 New York Avenue, N.W., 10th Floor  
Washington, D.C. 20530  
Telephone: (202) 514-1263  
Email: Woo.Lee@usdoj.gov

Attorneys for Plaintiff:  
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, ) Civil No. 3:20-cv-00126-JMK  
Plaintiff )  
 )  
 v. )  
 )  
 )  
FUND IN THE AMOUNT OF )  
73,293,750 AED (APPROXIMATELY )  
\$20 MILLION) IN THE POSSESSION )  
AND CONTROL OF RAS AL )  
KHAIMAH INVESTMENT AUTHORITY )  
(RAKIA) )  
 )

and )  
 )  
ALL CLAIMS FILED AND ASSERTED )  
BY VI2 PARTNERS GMBH AGAINST )  
RAS AL KHAIMAH INVESTMENT )  
AUTHORITY GEORGIA LLC IN CASE )  
NO. 2b/4319-17 PENDING BEFORE )  
THE TBILISI COURT OF APPEALS, )  
REPUBLIC OF GEORGIA AND )  
PROCEEDS THEREOF, )  
 )  
Defendant *in rem.* )

## **COMPLAINT FOR FORFEITURE IN REM**

The United States of America, by its undersigned attorneys, brings this Complaint for Forfeiture *in Rem* and alleges as follows in accordance with Rule G(2) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions (the “Supplemental Rules”).

### **NATURE OF THE ACTION**

1. The plaintiff is the United States of America.
2. The defendants in this action (the “Defendant *Res*”) are funds in the amount of approximately 73,293,750 AED (the “Defendant Funds”) in the custody of the Ras Al Khaimah Investment Authority (“RAKIA”) in the United Arab Emirates (“UAE”) as well as a legal claim (the “Defendant Claim”) for the Defendant Funds filed and asserted by VI2 Partners GmbH (“VI2”) in *VI2 Partners GmbH v. Ras Al Khaimah Investment Authority Georgia LLC* (Case No. 2b/4319-17), which is currently pending before the Tbilisi Court of Appeals in the Republic of Georgia (the “Georgia Action”). The Defendant Funds were deposited by VI2’s predecessors in interest while seeking to purchase a hotel in Tbilisi, Georgia, from its owner, the Ras Al Khaimah

Investment Authority Georgia LLC. The Georgia Action was filed by VI2 on or about February 19, 2016, seeking a return of the Defendant Funds and damages when the purchase of the hotel did not occur.

3. The only persons believed by the government to have an interest that may be affected by this action are VI2 and Ras Al Khaimah Investment Authority Georgia LLC, which is a wholly-owned subsidiary of RAKIA.

#### **NATURE OF THE ACTION**

4. This is a civil action *in rem* to forfeit assets involved in and traceable to an international conspiracy to launder funds traceable to violations of the International Emergency Economic Powers Act (“IEEPA”), 50 U.S.C. §§ 1701-1705, and a scheme to defraud financial institutions in the Republic of Korea (“Korea”). The United States of America seeks the forfeiture of the Defendant *Res* pursuant to 18 U.S.C. § 981(a)(1)(C), on the ground that it was derived from violations of U.S. and Korean law, and pursuant to 18 U.S.C. § 981(a)(1)(A) on the ground that the Defendant *Res* constitutes property involved in one or more money laundering offenses in violation of 18 U.S.C. §§ 1956 and/or 1957, and is property traceable to such property

#### **JURISDICTION AND VENUE**

5. This is a civil forfeiture action brought pursuant to 18 U.S.C. §§ 981(A) and (C).

6. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355.

7. Venue is proper in this district pursuant to 28 U.S.C. §§ 1335(b)(1)(A) and 1335(b)(2) because acts and omissions giving rise to the forfeiture took place in the District of Alaska.

**BACKGROUND: RELEVANT INDIVIDUALS AND ENTITIES**

8. **Kenneth Zong** is a U.S. citizen who formed multiple companies registered in Korea, including KSI Ejder Korea Inc. and Anchore. On December 15, 2016, Kenneth Zong was indicted in the District of Alaska for conspiracy to violate IEEPA, money laundering and money laundering conspiracy. The indictment alleges, among other things, that Zong and others allegedly conspired to evade the prohibitions of IEEPA and the Iranian Transactions and Sanctions Regulations (“ITSR”) by engaging in false, fictitious and fraudulent transactions which were designed to unlawfully convert and remove Iranian owned funds, equivalent to approximately \$1 billion U.S. dollars (“USD”). These funds were held in Korean bank accounts and converted into more easily tradeable currencies, such as USDs and/or euros, by deceiving Korean banks and regulators into thinking the transactions were legitimate. On or about February 6, 2013, Zong was also convicted in Korea of violations of Korea’s Foreign Exchange Transaction Act and customs laws in connection with his operation of KSI, and sentenced to two years imprisonment. Zong remains in Korea.

9. **Pourya Nayebi** is an Iranian national and born on July 25, 1974. In 2011, Nayebi, along with **Houshang Hosseinpour** and **Houshang Farsoudeh** (collectively the “Uncharged Conspirators”), acquired the majority of shares in a licensed bank in the Republic of Georgia with direct correspondent ties to other international financial institutions through a Liechtenstein-based foundation. The Uncharged Conspirators used the Georgia financial institution to facilitate transactions for multiple Iranian banks, including Bank Mellî, Mir Business Bank, Bank Saderat, and Bank Tejarat. On February 6, 2014, the U.S. Department of the Treasury designated the

Uncharged Conspirators as individuals subject to U.S. sanctions pursuant to Executive Orders 13224 and 13382. In announcing this designation, the Treasury Department stated that they and others subject to U.S. sanctions played a key role in evading U.S. sanctions on Iran.

10. **Houshang Hosseinpour** is an Iranian national and born on March 21, 1967.

11. **Houshang Farsoudeh** is an Iranian national and born on October 10, 1968. On February 6, 2014, Farsoudeh was designated by the U.S. Department of the Treasury as an individual subject to U.S. sanctions pursuant to Executive Orders 13224 and 13382.

12. **Anchore** is a legal entity registered in Seoul, Korea. It was originally formed by Kenneth Zong in 2009 as KSI Ejder Korea Inc. before Zong changed its name to Anchore in 2011.

13. **Orchidea Gulf Trading (“Orchidea Trading”)** is an entity based in the United Arab Emirates and owned by the Uncharged Conspirators. On February 6, 2014, Orchidea Trading was designated by the U.S. Department of the Treasury as an entity subject to U.S. sanctions pursuant to Executive Orders 13224 and 13382.

14. **MSL & Co. (“MSL”)** is another entity controlled by the Uncharged Conspirators. MSL was originally based in the UAE. At an unknown date, MSL changed its name to European Oil Traders SA and moved its location to Niederglatt, Switzerland. On February 6, 2014, European Oil Traders was designated by the U.S. Department of the Treasury as an entity subject to U.S. sanctions pursuant to Executive Orders 13224 and 13382.

15. **Industrial Bank of Korea (“IBK”)** is a financial institution in the Republic of Korea where the Central Bank of Iran maintained an account that at one time possessed a balance of over \$1 billion USD (the “CBI Won Account”).

16. **Ras al Khaimah Investment Authority (“RAKIA”).** RAKIA is an industrial licensing and promotion agency owned by Ras al Khaimah intended to promote investments in the Emirate of Ras al Khaimah, one of the seven emirates that make up the UAE. RAKIA is currently in possession of the equivalent of approximately \$20 million of funds paid to RAKIA by the Uncharged Conspirators in connection with a failed attempt to purchase a hotel owned by RAKIA in the Tbilisi, Georgia (the “Tbilisi Hotel”).

17. **VI2 Partners GmbH (“VI2”)** is an Austrian legal entity owned by Marc-Milo Lube, an Austrian national. VI2 alleges in the Georgia Action it filed against RAKIA that it owns and acquired from the Uncharged Conspirators any interest and/or claim the Uncharged Conspirators formerly possessed against RAKIA in connection with their failed attempt to purchase the Tbilisi Hotel.

#### **EVIDENCE SUPPORTING FORFEITURE**

18. The Defendant *Res* represents the proceeds of more than \$1 billion in Korean Won (“KRW”) converted into U.S. dollars in or through U.S. financial institutions in violation of IEEPA. The funds were then further transferred and laundered by Zong, a U.S. citizen—at the direction of the Uncharged Conspirators—through a web of shell company accounts at financial institutions in several jurisdictions, including the UAE.

#### **FACTS**

##### **I. U.S. AND KOREAN SANCTIONS ON IRAN**

19. U.S. law prohibits any U.S. person, including financial institutions inside the United States, from providing services directly or indirectly to Iran or the Government of Iran, in

the absence of a license from the U.S. Department of the Treasury, Office of Foreign Assets Control (“OFAC”). This prohibition includes the unlicensed processing of transactions through U.S. banks that are for the benefit of the Government of Iran, including any agency or instrumentality of the Government of Iran or any entity owned or controlled by the Government of Iran. The Central Bank of Iran (“CBI”) is part of the Government of Iran and has been identified by OFAC as an entity owned or controlled by the Government of Iran since prior to 2000.

20. The International Emergency Economic Powers Act (50 U.S.C. §§ 1701 et seq.) authorizes the President “to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States” by declaring a national emergency with respect to such threats, 50 U.S.C. § 1701(a), and to take steps to address such threats, including the authority to “investigate, regulate, or prohibit . . . any transactions in foreign exchange,” “transfers of credit or payments between, by, through, or to any banking institution, to the extent that such transfers or payments involve any interest of any foreign country or a national thereof,” and “the importing or exporting of currency or securities by any person, or with respect to any property, subject to the jurisdiction of the United States[,]” 50 U.S.C. § 1702(a)(1)(A).

21. Beginning with Executive Order No. 12170, issued on November 14, 1979, the President found that “the situation in Iran constitutes an unusual and extraordinary threat to the national security, foreign policy and economy of the United States and . . . declare[d] a national emergency to deal with that threat.” On March 15 and May 6, 1995, the President issued

Executive Orders Nos. 12957 and 12959, prohibiting, among other things, the exportation, reexportation, sale, or supply, directly or indirectly, to Iran of any goods, technology, or services from the United States or by a United States person, and on August 19, 1997, issued Executive Order No. 13059 clarifying the previous orders (collectively, the “Executive Orders”). The Executive Orders authorized the United States Secretary of the Treasury to promulgate rules and regulations necessary to carry out the Executive Orders. Pursuant to this authority, the Secretary of the Treasury promulgated the Iranian Transactions Regulations (renamed in 2012 the Iranian Transactions and Sanctions Regulations, or “ITSR”) implementing the sanctions imposed by the Executive Orders.

22. The ITSR, Title 31, Code of Federal Regulations, Section 560.204, prohibit, among other things, the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, of goods, technology, or services to Iran or the Government of Iran (with certain limited exceptions), including the exportation, reexportation, sale or supply of goods, technology or services to a third country knowing that such goods, technology or services are intended for Iran or the Government of Iran, without a license from OFAC. The ITSR provide that the transfer of funds, directly or indirectly, from the United States or by a U.S. person to Iran or the Government of Iran is a prohibited export, reexport, sale, or supply of services to Iran or the Government of Iran. See 31 C.F.R. § 560.427(a). The ITSR further prohibit transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate the ITSR. 31 C.F.R. § 560.203.

23. OFAC also maintains the Foreign Sanctions Evaders List (“FSE List”) to identify foreign persons sanctioned under Executive Order 13608, “Prohibiting Certain Transactions With and Suspending Entry Into the United States of Foreign Sanctions Evaders With Respect to Iran and Syria.” This FSE List includes persons sanctioned pursuant to Executive Order 13608 for engaging in conduct relating to the evasion of United States economic and financial sanctions with respect to Iran or Syria.

24. In 2010, Congress also enacted The Comprehensive Iran Sanctions Accountability and Divestment Act of 2010 (“CISADA”), which, among other things, authorized the imposition of sanctions against foreign financial institutions that engaged in transactions either facilitating Iran’s nuclear or ballistic missiles programs, or with persons and entities designated under United Nations and U.S. sanctions against terrorism and weapons of mass destruction proliferation.

25. In addition to U.S. sanctions, Korea also imposed its own bilateral sanctions on Iran beginning on or before 2011. The Korean government, in consultation with the United States Government, authorized IBK and another Korean bank to each establish a Korean won (“KRW”)-denominated account belonging to the Central Bank of Iran.

26. In 2011, the Central Bank of Iran maintained an account at IBK in Seoul containing the equivalent of over \$1 billion in KRW (the “CBI Won Account”). The purpose of this account was to permit limited forms of trade between Korea-based entities and Iran, including the import of Iranian oil to Korea. The CBI Won Account at IBK was subject to several limitations. Among other things, the account could be used for transactions involving only certain, permissible types of goods, including crude oil exports from Iran. The CBI Won Account could also be used to

compensate Korean businesses who were owed compensation from Iran for certain types of limited and permissible commercial trade and sales actions. All other transactions – including transactions for weapons — were specifically prohibited. Additionally, transactions involving the CBI Won Account could not involve USD.

**II. THE SCHEME TO FRAUDULENTLY CONVERT CBI ACCOUNT FUNDS**

27. Beginning on or before 2011 and continuing thereafter, Kenneth Zong and the Uncharged Conspirators, namely—Pourya Nayebi, Houshang Hosseinpour, and Houshang Farsoudeh – conspired to convert KRW held in the CBI Won Account into USD and other currencies, and to launder those funds in and through accounts held by multiple shell companies, including Orchidea Trading, in several jurisdictions, including the UAE.

28. In furtherance of this scheme, Zong and his associates orchestrated a complex scheme to defraud Korean banks, including IBK. Zong and his associates fraudulently represented to IBK and other Korean banks that Anchore, a Korean company Zong controlled in Seoul, had sold hundreds of millions of dollars' worth of permitted commercial goods and services to Iran. In truth, no such transactions had ever taken place. Rather, these false representations were made to IBK in order to cause IBK to transfer funds from the CBI Won Account to Anchore's account at IBK, where Zong then—at the direction of the Uncharged Conspirators—wire transferred the proceeds of this deceptive and illegal scheme to multiple shell company accounts in several other jurisdictions, including the UAE.

29. In total, between February 10, 2011 and July 20, 2011, Zong initiated over 88 transactions via IBK accounts, thereby causing \$1,004,662,911.57 worth of Iranian funds to be

transferred by IBK's CBI Won Account to accounts Zong controlled, converted to USD, and transferred by IBK at Zong's direction to other accounts that Zong and his co-conspirators, the Uncharged Conspirators, controlled and/or for their benefit, all in violation of U.S. sanctions laws.

30. As explained below, approximately \$20 million of these funds were used by the Uncharged Conspirators in attempting to purchase the Tbilisi Hotel in the Republic of Georgia, and \$10 million was transferred to bank accounts controlled by Zong and his relatives at financial institutions in Anchorage, Alaska.

**A. ZONG REPRESENTED FALSELY TO IBK THAT KSI/ANCHORE SOLD MARBLE TILES TO IRAN IN ORDER TO WITHDRAW OVER \$2 MILLION IN FUNDS FROM THE CBI WON ACCOUNT**

31. In or around July 2009, Kenneth Zong registered a company named KSI Ejder Korea Inc. ("KSI") in Seoul, Korea. On or about January 25, 2011, Zong opened a bank account at IBK in KSI's name. In or around February 2011, Zong changed KSI's name to Anchore.

32. Beginning in at least January 2011, Zong and the Uncharged Conspirators manufactured a host of commercial documents fraudulently representing that Anchore acquired \$2 million worth of marble tiles and other construction supplies from MSL and sold and exported these goods to Farsoodeh and Partnership ("Farsoodeh"), an Iranian company located on Kish Island in Iran.

33. In truth, Anchore never sold or delivered any marble tiles or construction materials to Farsoodeh. Nor did Anchore acquire any marble or construction materials from MSL. In fact, Zong and the Uncharged Conspirators fabricated and backdated all of the above commercial documents to give the appearance that Anchore was engaged in legitimate commercial

transactions with Farsoodeh and MSL. Zong emailed an associate of the Uncharged Conspirators on or about February 1, 2011, explaining:

*Let's do this way.*

*UAE company issues an OFFER SHEET to KSI EJDER KOREA INC then I will issue a Commercial INVOICE to Farsoodeh & Partnership Co. based on UAE Offer sheet. OFFER sheet must be back dated Jan 17, 2010 and description of commodity is various different kinds of Italian Marbel Tile, finished in UAE (which country ?) Offer sheet must be lower amount than INVOICE amount. Invoice amount shall be KRW2,650,000,000.- OFFER price should be USD2,303,347.80 (or similar). it shows KSI EJDER makes a little profit, Again this is just paper works for to get approval from Korea Central bank.*

*Regards/ken”*

34. Between January 27 and 28, 2011, within three days of opening the Anchore account at IBK, Zong presented the above fraudulent commercial contracts and invoices to IBK in order to justify and receive authorization to accept two monetary transfers from the CBI Won Account—one for ₩2,000,000,000 KRW and a second for ₩650,000,000 KRW—to Anchore’s account at IBK. The transfers were executed by IBK after Zong presented the fraudulent invoices and contracts to IBK and Iranian financial institutions, in turn, tendered payments requests to IBK to transfer CBI Won Account funds to pay Anchore’s invoices.

**B. ZONG REPRESENTED FALSELY TO IBK THAT ANCHORE SOLD HUNDREDS OF MILLIONS OF DOLLARS IN ADDITIONAL CONSTRUCTION MATERIALS TO IRAN TO WITHDRAW THE EQUIVALENT OF OVER \$1 BILLION FROM THE CBI WON ACCOUNT**

35. In or around May 2011, Zong tendered additional fraudulent documents to IBK and the Korean government in order to obtain hundreds of millions of dollars in additional transfers from the CBI Won Account. Specifically, Anchore represented fraudulently that it possessed a

contract dated February 2011 to supply Farsoodeh with additional construction materials, including “Heavy duty Galvazined Steel, Custom pre-colored Window & [W]ood frame[s].”

36. In or around May 2011, Anchore also submitted an application to the Korean government requesting permission to engage in this type of trade with Iran. According to Zong, the value of the materials to be supplied to Iran was \$15,605,704,000. In reality, however, Anchore never acquired nor exported any such construction materials to Iran.

37. In order to supply construction materials to Farsoodeh, Zong claimed that he would purchase these materials from Orchidea Trading, a UAE entity controlled by the Uncharged Conspirators—the same individuals who also owned Farsoodeh.

38. Notwithstanding the fact that Anchore never sold any construction materials to Farsoodeh, and Anchore acquired no materials from Orchidea Trading, Zong requested that IBK utilize funds in the CBI Won Account to pay him the equivalent of hundreds of millions of dollars in compensation.

39. Based upon fraudulent commercial invoices and contracts Zong presented to IBK, the equivalent of more than \$1 billion in KRW was transferred from the CBI Won Account to Anchore’s account at IBK between February and July 2011.

40. Zong deceived IBK regarding the transactions. Zong concealed material facts, for example, that Orchidea Trading, where the vast majority of the CBI Won Account funds were sent, was controlled by the same individuals that owned Farsoodeh—namely, the Uncharged Conspirators.

a. For instance, in manufacturing fraudulent contracts between Anchore and Orchidea, an associate of the Uncharged Conspirators (“Iranian Associate A”) advised Zong to remove any references to Farsoodeh in Anchore’s contracts with Orchidea in order to avoid “problems” with Orchidea’s banks in the UAE. On or about June 6, 2011, Zong received an email from Iranian Associate A stating:

*We can only make the [contract] direct with Anchore and Orchidea. As if we involve any Irani company like Farsoodeh in our contract then our banks in UAE will creat problems for us. So isnt this possible that we do contracts same as before. One contract between Farsoodeh and Anchore , and second one between Orchidea and Anchore[?]*

b. Similarly, Houshang Hosseinpour also reiterated to Zong the importance of not disclosing how Zong would utilize the CBI Won Account funds once they were released to him by IBK. In an email to Zong, Hosseinpour wrote: “Iran now is bad situation. If any swift will come back to iran.our road will be close.” Hosseinpour copied Orchidea Trading’s email address on this email. In a later email, Hosseinpour confirmed to Zong, “we got green light from Iran.”

41. Upon receiving these funds, Zong caused some of these funds to be exchanged for U.S. dollars and wired—at the direction of the Uncharged Conspirators—to nearly four dozen different persons and entities in several jurisdictions, including, among other places, the United States, the UAE, Switzerland, Canada and Bahrain. The funds were directed as follows:

- a. Approximately \$863 million was sent to accounts maintained in the name of Orchidea Trading at Emirates Bank in the UAE;
- b. Approximately \$131,000,000 was transferred cumulatively to other shell company accounts in the U.A.E.;

- c. \$10,564,572 was transferred cumulatively to twenty different individuals and four companies in the United States, including Alaska;
- d. Approximately €469,978 EUR (approximately \$668,825 equivalent) was transferred cumulatively to three companies in Italy;
- e. €299,653 EUR (approximately \$426,436 equivalent) was transferred cumulatively to six companies in Germany;
- f. €233,580 EUR (approximately \$332,407 equivalent) was transferred cumulatively to two companies in Switzerland;
- g. €97,000 EUR (approximately \$138,040 equivalent) was transferred cumulatively to a company in Austria;
- h. €56,000 EUR (approximately \$79,693 equivalent) was transferred cumulatively to an individual and one company in France;
- i. €32,480 EUR (approximately \$46,222 equivalent) was transferred cumulatively to a company in the Netherlands;
- j. \$40,000 was transferred cumulatively to an individual and one company in Canada; and
- k. \$30,000 was transferred cumulatively to two individuals in Bahrain.

42. As compensation for participating in this fraudulent scheme to funnel the equivalent of more than \$1 billion from the CBI Won Account to overseas accounts controlled by or for the benefit of the Uncharged Conspirators, Zong received an amount equivalent to approximately \$10 to 17 million as compensation. Approximately \$10 million of these funds were wired and deposited by Zong in a financial institution in Anchorage, Alaska.

//

//

**C. APPROXIMATELY \$20 MILLION IN FUNDS TRACEABLE TO THE CBI WON ACCOUNT WERE UTILIZED TO ATTEMPT TO PURCHASE THE TBILISI HOTEL**

43. As described below, the Uncharged Conspirators used \$20 million in funds traceable to the fraudulently procured CBI Won Account funds in attempting to purchase the Tbilisi Hotel in Georgia from RAKIA. The Uncharged Conspirators paid the equivalent of approximately \$20 million to RAKIA, the Tbilisi Hotel's owner.

44. Between October 2011 and March 2012, Houshang Hosseinpour, among others, engaged in discussions with RAKIA to purchase the Tbilisi Hotel. On or about March 1, 2012, New York Exchange LLC, an entity owned by the Uncharged Conspirators and whose chairman was Houshang Hosseinpour, and RAK Hotel, a subsidiary of RAKIA, entered into a share purchase agreement ("SPA"). Rak Hotel agreed in the SPA to sell the Tbilisi Hotel to New York Exchange LLC for approximately \$62.5 million.

45. Pursuant to the SPA, New York Exchange LLC agreed to make an initial deposit equivalent to approximately \$20 million with RAKIA. Between on or about October 12, 2011, and March 28, 2011, the Uncharged Conspirators tendered to RAKIA a series of checks drawn on multiple accounts maintained in the UAE in the names of various shell companies they controlled, including Orchidea Trading, New York General Trading LLC<sup>1</sup> and Tansam General Trading (New York General Trading LLC's former name). Specifically, RAKIA deposited the

---

<sup>1</sup> On February 6, 2014, New York General Trading LLC was designated by the U.S. Department of the Treasury as being subject to sanctions and was placed on OFAC's FSE List. In announcing the designation, the Treasury Department stated that New York General Trading LLC was an entity owned and/or controlled by the Uncharged Conspirators and was one of several front companies used "to deceive the international community ... by generating false invoices in connection with transactions involving designated Iranian banks."

following checks it received from the Uncharged Conspirators in connection with the SPA: (i) an Orchidea Trading check dated October 12, 2011, for 2.2 million AED; (ii) an Orchidea Trading check dated October 17, 2011, for 2 million AED; (iii) a check drawn on a New York General Trading LLC account dated October 19, 2011, for 10,478,000 AED; (iv) a check drawn on a New York General Trading LLC account dated November 16, 2011, for 8,257,500 AED; (v) a check drawn on a New York General Trading LLC account dated December 14, 2011, for 11,453,125AED; (vi) a check drawn on a New York General Trading LLC account dated December 28, 2011, for 11,453,125AED; (vii) an Orchidea Trading check dated March 19, 2012, for 725,000 AED; (viii) an Orchidea Trading check dated March 28, 2012, for 13 million AED; and (ix) an Orchidea Trading check dated March 28, 2012, for 13.25 million AED.

46. Upon receiving these checks, RAKIA deposited the funds into its account at the Commercial Bank of Dubai in the UAE. Those funds comprise the Defendant Funds in this action.

47. After negotiations between the Uncharged Conspirators and RAKIA terminated without being able to successfully conclude a final purchase agreement for the Tbilisi Hotel, VI2 Partners GmbH (“VI2”), an Austrian legal entity owned by Marc-Milo Lube, filed civil claims (the “Defendant Claim”) against RAKIA (the “Georgia Action”) in the Tbilisi City Court seeking, among other things, the return of all funds provided to RAKIA by Orchidea Trading, New York General Trading LLC and Tansam General Trading in connection with the SPA as well as additional damages allegedly caused by RAKIA. In filing its action, VI2 asserted that it had acquired the cause of action from Orchidea Trading, New York General Trading LLC and Tansam General Trading pursuant to a claim purchase agreement.

48. The Defendant Claim was filed by VI2 on or about February 19, 2016. After the Tbilisi Court issued a ruling in VI2's favor, RAKIA appealed the decision of the Tbilisi City Court to the Tbilisi Court of Appeal.

**FIRST CLAIM FOR RELIEF**

49. Paragraphs 1 through 49 above are incorporated by reference as if fully set forth herein.

50. The Defendant Funds and Defendant Claim (collectively, the "Defendant *Res*") is property that constitutes, and is derived from, proceeds traceable to one or more violations of IEEPA and foreign bank fraud, which are specified unlawful activities under 18 U.S.C. §§ 1956(c)(6)(B)(iii), 18 U.S.C. §§ 1956(c)(7)(A), 1956(c)(7)(B)(iv) and/or 1956(c)(7)(D).

51. The Defendant *Res* is, therefore, subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

**SECOND CLAIM FOR RELIEF**

52. Paragraphs 1 through 52 above are incorporated by reference as if fully set forth herein.

53. The Defendant *Res* is involved in, or is traceable to property involved in, one or more transactions or attempted transactions in violation of section 18 U.S.C. § 1957 and a conspiracy to commit such offenses in violation of section 18 U.S.C. § 1956(h). Specifically, the Defendant *Res* was involved in or is traceable to property involved in one or more financial transactions, attempted transactions, and a conspiracy to conduct or attempt to conduct such

transactions in criminally derived property of a value greater than \$10,000 that was derived from specified unlawful activities, namely: IEEPA and foreign bank fraud.

54. The Defendant *Res* is, therefore, subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

**THIRD CLAIM FOR RELIEF**

55. Paragraphs 1 through 55 above are incorporated by reference as if fully set forth herein.

56. The Defendant *Res* is involved in, or is traceable to property involved in, one or more transactions, or attempted transactions in violation of section 18 U.S.C. § 1956(a)(1)(B)(i) and a conspiracy to commit such offenses in violation of section 18 U.S.C. § 1956(h). Specifically, the Defendant Asset is involved in and is traceable to property involved in one or more financial transactions, attempted transactions, and a conspiracy to conduct or attempt to conduct such transactions involving the proceeds of specified unlawful activity, that is: (i) violations of IEEPA (50 U.S.C. §§ 1701-1705); and (ii) a foreign offense involving fraud by or against a foreign bank (18 U.S.C. § 1956(c)(7)(B)(iii)); and were designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership or the control of the proceeds of the specified unlawful activities in violation of 18 U.S.C. § 1956(a)(1)(B)(i).

57. The Defendant *Res* is therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

//

//

**FOURTH CLAIM FOR RELIEF**

58. Paragraphs 1 through 57 above are incorporated by reference as if fully set forth herein.

59. The Defendant *Res* was involved in, or is traceable to property involved in, one or more transactions or attempted transactions in violation of section 18 U.S.C. § 1956(a)(2)(B) and a conspiracy to commit such offenses in violation of section 18 U.S.C. § 1956(h). Specifically, the Defendant Asset was involved in and are traceable to funds that were and were attempted to be, transported, transmitted, or transferred, and a conspiracy to transport, transmit, or transfer, to a place in the United States from or through a place outside the United States, with the knowledge that the funds involved in the transportation, transmission, or transfer represented the proceeds of some form of unlawful activity and knowledge that such transportation, transmission, or transfer was designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activities, that is: (i) violations of IEEPA (50 U.S.C. §§ 1701-1705); and (ii) a foreign offense involving fraud by or against a foreign bank (18 U.S.C. § 1956(c)(7)(B)(iii)).

60. The Defendant *Res* is therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

WHEREFORE, plaintiff United States of America prays that:

- (a) due process issue to enforce the forfeiture of the Defendant *Res*;
- (b) due notice be given to all interested parties to appear and show cause why forfeiture should not be decreed;

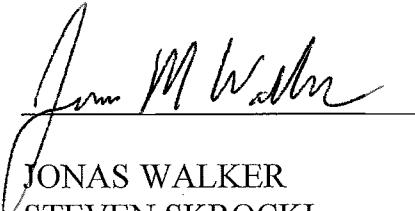
- (c) this Court decree forfeiture of the Defendant *Res* to the United States of America for disposition according to law; and
- (d) for such other and further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: June 3, 2020

Respectfully submitted,

BRYAN SCHRODER  
United States Attorney  
DEBORAH L. CONNOR  
Chief  
Money Laundering & Asset Recovery Section  
U.S. Department of Justice

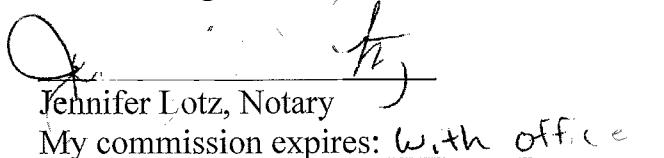
By:



JONAS WALKER  
STEVEN SKROCKI  
Assistant U.S. Attorney  
District of Alaska  
WOO S. LEE  
Deputy Chief, MLARS  
MICHAEL OLMSTED  
Sr. Trial Attorney, MLARS  
U.S. Department of Justice

Attorneys for Plaintiff  
UNITED STATES OF AMERICA

Subscribed before me on June 3, 2020, in Anchorage, Alaska,



Jennifer Lotz, Notary  
My commission expires: With office

**VERIFICATION**

I, Benjamin R. Mattson, hereby verify and declare under penalty of perjury that I am a Special Agent with the Federal Bureau of Investigation, that I have read the foregoing Verified Complaint for Forfeiture *In Rem* and know the contents thereof, and that the matters contained in the Verified Complaint are true to the best of my knowledge and belief.

The sources of my knowledge and information and the grounds of my belief are official files and records of the United States, publicly available files and historical information, information supplied to me by other law enforcement officers, experts, and other witnesses, as well as my investigation in this case, together with others, as a Special Agent of the Federal Bureau of Investigation.

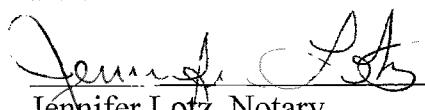
I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed June 3, 2020, at Anchorage, Alaska.



Benjamin R. Mattson  
Special Agent  
Federal Bureau of Investigation

Subscribed before me on June 3, 2020, in Anchorage, Alaska.



Jennifer Lotz, Notary  
My commission expires: With office

